Poornima Journal of Engineering Science & Management
*Vol. 1, Issue 1, 2024, pp 23-29, ISSN: ****-******

Cyber Attacks: A New Digital Weapon and Security Threats

Imran Mirza[1*], Mohammad Firdos Sheikh[1]
Department of Computer Science Engineering, Poornima University, Sitapura, Jaipur, Rajasthan, India

*Author to whom correspondence should be addressed:
E-mail: imranmirza100@gmail.com

Abstract: The whole world is developing at a faster rate and advancing which became possible because of computers. The internet is the backbone of this development. The idea of the internet was born in 1961. Then lots of people contributed to the idea but for the common man, it was in 1991 when Tim Berners Lee invented the World Wide Web (www). In the following years, almost every part of the world was connected to each other by the internet. But this tranquility came with a cost of integrity and security of information exchange and data. Today, almost every individual is generating, exchanging and storing data but threats of the breach always haunt people who have sensitive and confidential data. Every day cyber-attacks are carried out successfully and a lot of people, organizations, and companies suffer financial losses and integrity. In this paper, the study was carried out to show the successful attacks carried out all over the world for a period of two years spanning from 2015 to 2016 and point out the sectors and countries which were affected the most. We also classified the attacks in three classes based on the nature of their action. This helps to understand the course of action that can be taken to mitigate the effects of attack. This study highlights the void in the security of wireless sensor networks. This study also highlights the significance of security in wireless sensor networks.

Keywords: Cyber-attack, Wireless Sensor Networks, Security Issues, Network security.

1. Introduction

We live in a world where we are surrounded by sophisticated machines and automated systems which can work continuously 24 hours a day. One such machine which changed the fate of mankind was a computer. First, the computer was used for quick calculations for which it was invented, of course. The biggest hop in the run of development and modernization took when the computer was amalgamated with the internet. Then security measures came into existence to tackle these problems. Today the cyber-attacks and their countermeasures are neck-to-neck in competition. Researchers find a solution to one problem and intruders come with another method of intrusion. Firewalls were the only means of defense for the security of networks in early times, the first cyber-attack and intrusion was done by Morris Worm on 02/11/1988 in Send mail program[1] Since then the whole world is suffering from the menace of cyber-attacks but some countries suffer the most. These attacks are no doubt with a proper motive and aim. This motive could be anything ranging from ransom to terrorism. After firewalls, intrusion detection came into picture and standard of security increased. The concept of intrusion detection system was put forth by James P. Anderson in 1980. Cyber-attack detection is “the act of identifying persons who are using a system unauthorized and those legitimate users who misuse their privileges [2]. Both the fields got advanced, Intrusions and Intrusion detection systems. Cyber-attacks continue to be a nightmare for every individual and sector whose operations have computer networks involved. Actually, every sector is influenced by computer networks nowadays.

Lot of work has been done in developing IDS over the years to counter the problem of cyber-attacks and there is still a long way to go. It is very difficult to point out some particular and prominent contributions in this field but we still pointed out some work with more impact than others or we can say the works which set the base and standard for other researchers to work on like we have Bro, a stand-alone system for detecting network intruders in real-time. It emphasizes high-speed (FDDI-rate) monitoring, real-time notification, clear separation between mechanism and policy, and extensibility[3]. Mehiar Dabbagh et al.[4] proposed a method to detect slow port scanning and this method comprises of two stages: feature collection phase in which network traffic is analyzed to extract features needed to classify IP’s into malicious or not. Classification phase, based on collected features, divides IP’s into three groups: Normal, Suspicious and Scanner IP’s. Suspicious IP’s are monitored for next (k) time windows. In 1998 Martin Roesch created a system Snort. On IP networks it performs real-time analysis and logging of packets. Snort can be configured into packet sniffer, packet logger and intrusion detection mode[5]. The cluster center and nearest neighbor (CANN) approach was proposed by Wei-chao Lin et al. The distance between each data sample and its cluster center, and the second distance is between the data and its nearest neighbor in the same cluster are measured and summed, Then k-Nearest Neighbor (k-NN) classifier

detects intrusion by this new and one-dimensional distance-based feature which represents each data sample [6].

2. Classification of Cyber Attacks

We have classified the cyber various attacks in three classes based on the nature of damages they do:

a) Modifiers: modifiers are those attacks which have only one purpose and that is to modify original data. These attacks do not crash or damage the system but they compromise the integrity of the system. For example, IP spoofing, man-in-the-middle, compromised-key attack etc.

b) Analyzers: these attacks do not damage the system instead they compromise the confidentiality and integrity of information exchange. These attacks are dangerous because neither sender nor receiver is aware of it. The data remains as it is but the cloak of its secrecy and confidentiality gets breached. For example, sniffer attack, eavesdropping, etc.

c) Damagers: these attacks are just meant to destroy the system or services. These attacks do not intend to gain any profit from services or data to be targeted rather their sole intention is to damage the system or service as much as possible. Sometimes people damage a system or services in order to get the victims sever down so that the attacker's service gets more visitors. Service can be anything, like a website offering a service to download movies. For example, DOS attack, DDOS etc.

3. Detection Methodologies

Different strategies were given by different researchers to tackle the plague of cyber-attacks. These strategies were divided into two classes:

a) Anomaly-based detection: Anomaly detection technique works to find patterns that deviate from the normal and those are flagged as an intrusion [7]. In anomaly detection regular activities are referenced as normal behavior and any suspicious or any activity which does not fall under normal routine or behavior is considered an intrusion or attack. There are two general approaches to anomaly detection: specialized detection algorithms that target a particular type of anomalies, and generalized traffic profiling algorithms [8].

b) Signature-Based Detection: Signature-based detection attempts to detect attacks that follow a definite intrusion pattern. Such marking is gathered from known attacks and stored in the form of signatures in the database [4]. Because of the very common signatures and poorly built-in verification tool to authenticate the success of the attack, Signature-based IDS produce more false alarms than presumed [9]. This is the main cause that the researchers are fond of anomaly detection. This drawback of signature-based detection forces researchers to work on anomaly detection, which can detect unknown attacks.

4. Cyber Attack Menace

The cyber-attacks are creating ruckus everywhere. One may think that the developing and underdeveloped countries are under siege, but that is absolutely wrong. In fact, the most developed countries are facing it most because a thief always targets a big and wealthy house, not a hut. To support this statement cyber-attack statistics of some developed and famous countries are provided.

In the year 2015, the USA faced 437 successful attacks. These are those attacks which were successful and reported, whereas in 2016 488 successful attacks were reported. The targets are random and range from government websites to online games. The government and military websites were hacked by rival nation hackers. Origin of only some attacks is known. In the year 2015 and 2016, the UK faced 80 and 53 successful attacks respectively. These attacks not only damage systems and service but they also come with a price. These attacks cost $385 billion globally per year. Cyber-attacks cost the UK between £18 billion ($30 billion)-£27 billion ($45 billion) a year and in the US that figure is estimated to be approximately $100 billion by the UK National Audit Office [10]. India being a developing country also faces a lot of cyber-attacks. The largest data breach in history took place in February 2014 when a cache of personal data containing credentials for 360 million accounts and 1.25 billion email addresses went up for sale on an online black market [11]. In 2015-16, India suffered from 104 successful attacks. India loses Rupees 34,110 crore annually. The attacks which India faces from Pakistan and vice versa are never for monetary rewards. The cyber war continues between the two nations at regular intervals. Most of the attacks are website defacements. On January 1, 2016, a hacker group by the name of Scorp!n Att@ck3r from Muslim cyber army hacked Goa University(unigoa.ac.in) and dumped 10380 records with hashed passwords[12]. Later on March 24, 2016, Trend Micro released the details of operation major, a Pakistan linked cyber espionage campaign against Indian military employees [13]. Same was returned by Indian hackers On January 8, 2016, In revenge for the death of Lt. Col. Niranjan Kumar, an Indian hacking group IBH defaced several Pakistani websites[14].

Like these countries, more or less every country faces the wrath of cyber-attacks. With increasing tensions between several countries, cyber-attacks are the tools used by people to let out anger on the rival nation. The interference of the USA in the Middle East has led to an increase in cyber-attacks. The USA has made more enemies than friends in the last century. In 2015 Russian intelligence reportedly breached NSA, stealing cybersecurity strategy and exposing the agency's Cyberwarfare strategy[14]. On another occasion, the network of Democratic National Committee was hacked by Russian government hackers and 23- page document of opposition research on Donald Trump[15]. Like this most of the countries face cyber-attacks from rival

nations. It is not like that attacks come only from outside of the country but domestic attacks hold a large portion of attacks. The attacks from inside a country are mainly targeted at educational, industrial online games, news traffic signals etc.

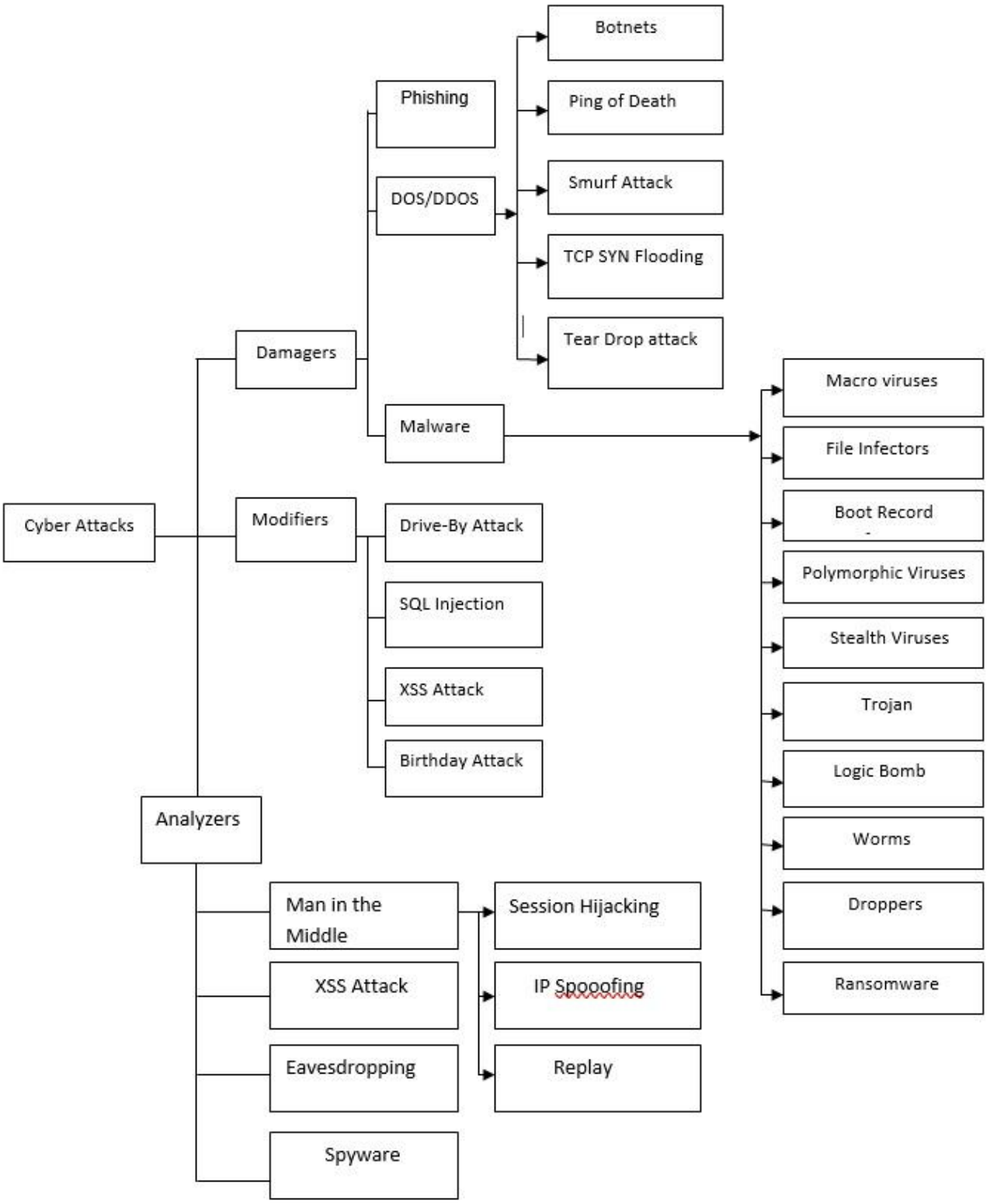

Figure 1. Classification of Cyber Attacks

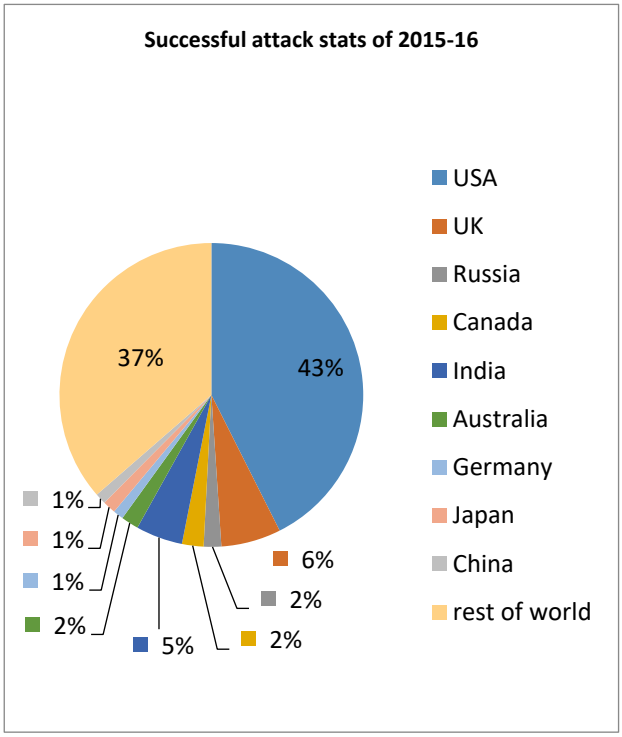

Figure 2. Successful reported Cyber Attacks of 2015 & 2016

It was on January 8, 2015, when a hacker group called Lizard Squad launched a DDoS attack against the imageboard site 8chan. This site was inaccessible throughout the United States [16]. In UK Blighty's government-funded educational network JANET was hit by a wave of DDoS Attacks on April 14, 2016[17]. Like these, there are thousands of cases around the world where websites of a country were hacked by its own citizens. By analyzing the cyber-attack data of 2015 and 2016, it was found that the major suffering country was the USA with 43% which is followed by the UK with 6%. The difference is huge and the cause behind it is diplomatic tensions between the US and some other nations. As per recent 2018 cyber-attack events on the US, the attacks were carried out mostly by Russia, China, and Iran [18]. The interfere of the USA in the middle east is the main cause of cyber-attacks from Iran on the US. Iran is continuously making efforts to launch cyber-attacks on the US. For example, after the 2016 elections in the US, Iranian attackers attempted to acquire information about the new administration and were also indulged in an attempt to compromise emails accounts of American team during nuclear negotiations [19].

5. Suffering Sectors

There is not a single area which has not suffered from the wrath of cyber-attacks. The intensity and frequency of attacks depend on the nature of the field. There are various factors which drive an intruder to attack a particular area or website. Those factors can be revenge, monetary gains, and personal interests, political message. It was on January 2nd, 2015 when a network of several Ukrainian Justice and Law Enforcement organizations were penetrated and some documents to proof the local level of corruption were leaked [20]. Apart from these reasons, there are hackers who hack a website just to prove their ability and disability of IT professionals operating and protecting those websites. Sometimes injustice force people to get involved in such acts, like a sexual assault case in Halifax Nova Scotia, Canada was re-opened by Halifax police after Anonymous exposes the identity of the alleged culprit on November 12th, 2015[21]. By the above discussion, we came to know that intrusion of any website depends on the motive and gains that an intruder is likely to get. However, there are some all-time hot and favorite targets which always offer some benefit to the intruder. These are regularly attacked around the globe. The frequent victim sectors include Industry at the top with 605 successful intrusions in 2015 and 2016 followed by. Analysis of data shows that Most of the times Government websites are hacked by rival nations to gain sensitive information or just to damage the website. On January 15, 2015, Dr.SHA6H continued his protest against the civilian killings in Syria by hacking official website of Perrysburg, Ohio (ci.perrysburg.oh.us)[22], before that official website of the Bundaberg library Australia was defaced on 11th of the same month and year by Dr. SHA6H[23]. As we saw in these attacks there is a clear motive of getting the attention of people over the crisis in Syria where innocent civilians are dying. Whatever be the cause and motive of a breach, it comes with a cost and that cost is in millions of dollars. It is estimated that by 2019 the global cost of cybercrime will touch $2 trillion. These costs include everything from ransomware to the cost of the system damaged and the loss of business because of the breach.

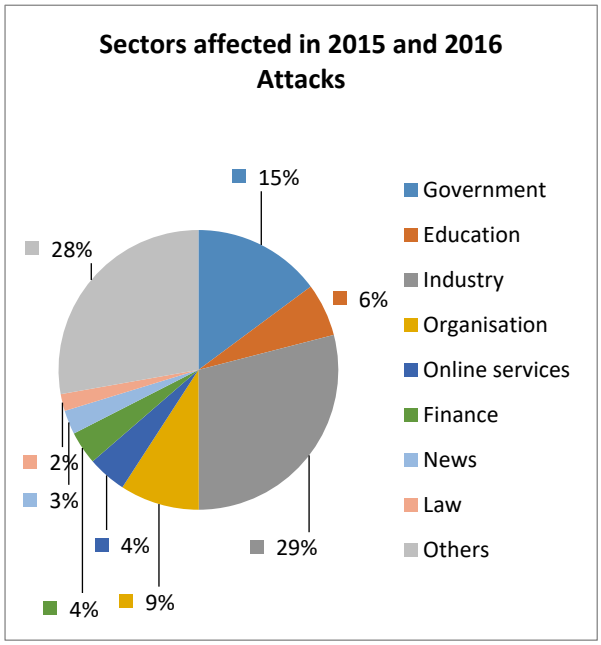

Fig.3. Various Sectors affected by Cyber-attacks in 2015 & 2016

The priority of sectors attacked depends on the goal of the attacker. If the goal of the attacker is to get the attention of people on social or humanitarian basis then he is likely to attack those sites which people visit most and most of the times the attack is a defacement of the website. Same like this if the attack is for monetary gains, then that sector is attacked which can pay the ransom, like an industrial sector or those websites which store data of clients. In political issues between nations, the websites are often defaced with some message. Figure 2 shows the major cyber affected sectors of 2015 and 2016. The government faces most of the attacks as compared to other sectors and attacked mostly by cyber espionage, cyber war and hacktivism [24].

5. Vulnerable Wireless

After the revolution of wired networks, the need to remain connected in mobility was felt and the first wireless network was developed under ALOHAnet in 1969 at the University of Hawaii, however, it became operational in 1971. The wireless technology broke the shackles and set free the wired slaves. The wireless technology kept on developing from WaveLAN product family in 1986 to the realm of 802.11ac latest wireless technology which introduced mankind to high-speed Gigabit Wi-Fi. Everything developed so fast except its security. Security of wireless networks developed at a snail's pace. It is not like that Wireless doesn't have security measures; it has but that is not enough as compared to wired networks. The popularity and usage of wireless networks require a lot more attention to security because it is replacing wired networks slowly and permanently. The wireless network makes it difficult to provide security as it is volatile. The attacker and victim are mobile and to identify an attacker is difficult. The motive of the attack is the same as that of a wired network. It has intrinsic signal defects as well as it is subject to interference from other electronic devices in its vicinity. Attacks on wireless networks are easy to perform. A simple example of such an attack is when a malicious node continuously transmits a radio signal and blocks any legitimate access to the medium or interferes with communication between sender and receiver. This process of interrupting communication is called jamming and jammers are those malicious nodes [25]. The wireless Physical layer is extremely vulnerable to eavesdropping and jamming attacks, the primary technique of MAC attacks is MAC spoofing, the IP spoofing, hijacking and Smurf attack are network-layer attacks which exploit IP weaknesses. In the transport layer TCP, UDP flooding and the TCP sequence number prediction attacks are common. The application-layer attacks can be categorized as HTTP attacks, FTP attacks, and SMTP attacks which include Malware attack, FTP bounce attacks, directory traversal attacks, password "sniffing," SMTP viruses, worms and e-mail spoofing [26]. The broadcasting nature of wireless channels makes wireless communication networks particularly vulnerable to eavesdropping and impersonation attacks.

6. Routing Attacks in Sensor Networks

The attacks that happen while routing messages and act on network layer are known as routing attacks. Some of the routing attacks are [27]:

a) Selective Forwarding of Packets: In this selective forwarding case the compromised or malicious node refuses to forward certainly selected packets. Otherwise, in sensor networks, the nodes forward packets which they receive [28].

b) Sinkhole: In this type of attack the traffic is attracted from a particular area to pass through a malicious node. An attacker makes the malicious node so attractive to the surrounding nodes that most of them fall into the trap [29].

c) Sybil: This attack targets the fault tolerant schemes like Multipath routing, Topology maintenance, and Distributed storage. In this attack, a single node duplicates itself and presents multiple identities to other nodes of the network [30].

d) Wormholes: In a wormhole attack Packets are tunneled to other location from one location where attacker records Packets and retransmitted from there [31].

e) Hello Flood: In this attack, the Hello packets of routing protocol are sent from one node to another with more energy. Hello, packets are sent to a number of isolated sensor nodes in WSN by an attacker with high radio transmission, range, and processing power. By this approach, the sensors are made to believe that adversary is their neighbor and victim nodes try to go through it while sending information hence they get spoofed [32].

All these attacks target different layers of the network, like sinkhole attack, and wormhole attack target link layer and network layer, Hello flood attack targets network layer, Sybill attack targets network layer, and application layer, while DoS attack targets physical, link, network and transport layers.

6. Routing Attacks in Sensor Networks

The Adhoc, wireless networks present a significant problem in designing Security schemes [27]. The main issues which contribute to its security shortcomings are:

a) Wireless Medium: the broadcast nature of wireless makes it vulnerable to various attacks like eavesdropping. The wireless medium allows an attacker to intercept and inject malicious code [33].

b) Adhoc Deployment: The Adhoc nature of wireless means no definite or permanent structure or topology [34]. The topology of the wireless network is always dynamic. It is subject to change because of various reasons like Node failure, an increase in the number of nodes and mobility of Nodes. So, in this dynamic environment, the security schemes should be able to function properly and Network must support self-configuration.

c) Inimical territory: Another challenging aspect is that

most of the times sensor nodes are deployed in unfavorable conditions where they are subject to catastrophic damage or may be captured by attackers to extract valuable data [35].

d) Limited resources: due to limited resources of sensor networks, the security schemes must not be resource hungry. The Memory, Power, and Bandwidth are limited so the security schemes must be efficient in all these areas.

e) Large Scale deployment: This dimension poses a significant threat to security. This is directly proportional to the threat of WSN. As the size of the network increases, the chances of a successful attack also increase. The schemes should be efficient enough to be applied to large wireless networks.

6. WSN Applications

a) Military Applications: Because of cost effectiveness, easy deployment and powerful capabilities of wireless sensors, these are must use in military operations [36]. WSN plays an important role in military operations, whether it is urban warfare, battlefield or Force protection. Some of the classes of military applications of WSN are Self-Healing Landmines, Soldier detection and tracking, Aerostat Acoustic Payload for Transient Detection, Early Attack Reaction Sensor, Perimeter Protection and many more [37].

b) Environmental Applications: The Wireless Sensors are an essential part of environmental monitoring. The application in Environmental monitoring ranges from sophisticated weather stations to cattle monitoring in a farm [38]. The wireless sensors are well capable of monitoring several environmental factors like humidity, rainfall, water velocity, temperature, air quality and many other aspects. WSN enable a long-term environmental monitoring with high precision, which is difficult by using conventional methods [39].

c) Healthcare: Healthcare sector is also a sector which employs wireless sensors to continuously monitor the health of a person. The parents to keep toddlers under surveillance also use it. The beneficiaries are mainly those who are unable to take care of themselves like elderly people, children and critically ill people [40].

d) logistic Support: As the companies are expanding all over the world, they are suffering a major problem of inventory control. The asset tracking by RFID tags and wireless sensor networks is the best possible solution to this problem. The companies are adapting to this method, which is proving fruitful.

6. Conclusion

The security of networks is the biggest issue and developed nations are spending billions of dollars on cyber security every year. Despite spending huge amounts on security, there is still a large void, which needs to be filled. This is evident from the statistics that were presented in (section 3, 4). The wireless sensor networks are recent advancement in the field of networking and so is its security in infancy. This shows the need for improvement in the security of WSN's as they are used in critical military applications, environmental applications, and various other important sectors. The unauthorized access or attacks in these networks could cause serious implications. For example, a Flood Early Warning System deployed at an important location to predict and warn the authorities about a possible flood is being compromised by an attacker, then the results would be devastating. In these kinds of attacks, the attacker could use a natural disaster as a weapon.

Acknowledgment

The concept and drafting were done by the first author. The co-author assisted in analysis of data, grammar checking and structuring the manuscript.

References

1. M. K. Asif and T. A. Khan, "Network Intrusion Detection and its strategic importance Network Intrusion Detection and its Strategic Importance," no. April, 2013.
2. J. Raiyn and B. Alqarbiah, "A survey of Cyber Attack Detection Strategies," vol. 8, no. 1, pp. 247–255, 2014.
3. V. Paxson and V. Paxson, "Bro: A System for Detecting Network Intruders in Real-Time Bro: A System for Detecting Network Intruders in Real-Time," 1998.
4. M. Dabbagh, A. J. Ghandour, K. Fawaz, W. El-Hajj, and H. Hajj, "Slow port scanning detection," Proc. 2011 7th Int. Conf. Inf. Assur. Secur. IAS 2011, pp. 228–233, 2011.
5. P. Mehra, "A brief study and comparison of Snort and Bro Open-Source Network Intrusion Detection Systems," vol. 1, no. 6, pp. 383–386, 2012.
6. W. Lin, S. Ke, and C. Tsai, "Knowledge-Based Systems CANN: An intrusion detection system based on combining cluster centers and nearest neighbors," Knowledge-Based Syst., vol. 78, pp. 13–21, 2015.
7. S. Vijayarani and M. Sylviaa, "Intrusion Detection System," Int. J. Secur. Priv. Trust Manag., vol. 4, no. 1, pp. 31–44, 2015.
8. D. Brauckhoff, B. Tellenbach, A. Wagner, M. May, and A. Lakhina, "Impact of packet sampling on anomaly detection metrics," Proc. 6th ACM SIGCOMM Conf. Internet Meas., vol. 24, no. 12, pp. 159–164, 2006.
9. M. M. Hassan, "Network Intrusion Detection System Using Genetic Algorithm and Fuzzy Logic," vol. 4, no. 2, pp. 1435–1445, 2013.
10. C. Kaul, "Analysis of the Cyber Attacks over the Past Decade," vol. 6, no. 2, pp. 40–43.
11. B. Watkins, "The Impact of Cyber Attacks on the Private Sector," no. August, 2014.

12. "Goa university hacked," 2016. [Online]. Available: http://opindiareborn.blogspot.co.uk/.
13. Waqas, "Espionage attack on Indian Military," 2016. [Online]. Available: https://www.hackread.com/pakistan-hackers-cyber-espionage-campaign-india-army/.
14. C. Cimpanu, "Defacement of pakistani websites by IBH," 2016. [Online]. Available: http://news.softpedia.com/news/indian-hackers-deface-pakistani-websites-as-homage-to-dead-soldier-s-daughter-498652.shtml.
15. E. Nakashima, "No Title," 2016. [Online]. Available: https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html.
16. S. Machkovech, "8chan, related sites go down in Lizard Squad-powered DDoS," 2015. [Online]. Available:https://arstechnica.com/information-technology/2015/01/8chan-related-sites-go-down-in-lizard-squad-powered-ddos/.
17. K. Hall, "JANET attacked by DDoS," 2016. [Online]. Available: http://www.theregister.co.uk/2016/04/18/janet_clobbered_with_ddos_attacks_again/%0A.
18. I. Studies, "Center for Strategic and International Studies (CSIS) | Washington, D.C.," no. December, 2018.
19. K. S. Collin Anderson, "Iran's cyber threat, espionage, sabotage and revenge," Carnegie Endow. Int. Peace Publ. Dep., 2018.
20. "network of ukranian Law enforcement and justice hacked," 2015. [Online]. Available: https://www.cyberguerrilla.org/blog/croatia-government-corruption-and-ukraine-prosecutor-general-office-massive-hack-leak-symantec-hackers/.
21. Waqas, "Halifax police forced to re-open sexual assualt case After anonymous exposes Identity of culprit.," 2015. [Online]. Available: https://www.hackread.com/anonymous-exposes-identity-of-alleged-halifax-rapist/.
22. Waqas, "Ohio city' Website Hacked by Free Syrian Hacker," 2015. [Online]. Available: https://www.hackread.com/ohio-city-website-hacked-by-free-syrian-hacker/.
23. C. Honnery, "Bundaberg Library hacked by DR. sha6h," 2015. [Online]. Available: http://www.couriermail.com.au/news/queensland/bundaberg-library-website-hacked-by-people-claiming-to-be-from-free-syrian-people/story-fnn8dlfs-1227181518953?nk=6e492609ecada6b9cfe30ae627da5a85
24. A. Bendovschi, "Cyber-Attacks – Trends, Patterns and Security Countermeasures," vol. 28, no. April, pp. 24–31, 2015.
25. K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of Service Attacks in Wireless Networks: The Case of Jammers," IEEE Commun. Surv. Tutorials, vol. 13, no. 2, pp. 245–257, 2011.
26. Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," Proc. IEEE, vol. 104, no. 9, pp. 1727–1765, 2016.
27. D. G. Padmavathi and M. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," Int. J. Comput. Sci. Inf. Secur., vol. 4, no. 1, pp. 1–9, 2009.
28. L. K. Bysani, "A Survey on Selective Forwarding Attack in Wireless Sensor Networks," 2011.
29. A. S. S, M. A. Razzaque, P. Naraei, and A. Farrokhtala, "Detection of Sinkhole Attack in Wireless Sensor Networks," no. July, pp. 1–3, 2013.
30. J. Grover, "A Sybil Attack Detection Approach using Neighboring Vehicles in VANET," pp. 151–158, 2011.
31. Z. A. Khan and M. H. Islam, "Wormhole Attack: A new detection technique," no. October 2012, 2015.
32. C. S. Issues, "International Journal of Computer Science Issues," vol. 7, no. 3, 2010.
33. F. Khan, "Secure Communication and Routing Architecture in Wireless Sensor Networks," pp. 647–650, 2014.
34. H. Jadidoleslamy, "A Comparison of Link L ayer Attacks on Wireless Sensor Networks," vol. 3, no. 1, pp. 35–56, 2011.
35. V. Kumar, A. Jain, and P. N. Barwal, "Wireless Sensor Networks: Security Issues, Challenges and Solutions" vol. 4, no. 8, pp. 859–868, 2014.
36. Selmic, Rastko R., Vir V. Phoha, and Abdul Serwadda. "Wireless Sensor Networks. New York, NY, USA: Springer International Publishing AG, 2016.vol. 2, no. 12, pp. 164–168, 2016.
37. M. Pejanovi and Z. Tafa, "A Survey of Military Applications of Wireless Sensor Networks," 2012.
38. B. P. Corke, T. Wark, R. Jurdak, W. Hu, P. Valencia, and D. Moore, "Sensor Networks," vol. 98, no. 11, 2010.
39. F. M. Al-turjman, H. S. Hassanein, and M. A. Ibnkahla, "Efficient deployment of wireless sensor networks targeting environment monitoring applications," Comput. Commun., vol. 36, no. 2, pp. 135–148, 2013.
40. H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey," Comput. Networks, vol. 54, no. 15, pp. 2688–2710, 2010.
41. Vaidya T. 2001-2013: Survey and Analysis of Major Cyberattacks. arXiv preprint arXiv:1507.06673. 2015 Jul 23.