Analysis of Information Security Issues in Computer Networks and Prevention Techniques using Wireless Sensor Networks

Nihal Kulkarni-101178458
Dept of Systems and Computer Engineering
Carleton University
Ottawa, Canada
nihalkulkarni@cmail.carleton.ca

Abstract -- **Computer network security has become a crucial element in the day-to-day life as world's scientific and technology level continues to rise. The computer networks not only increase the efficiency of communication systems, as well as minimize the commute time between people, and can also advance the global social and economic development, resulting in a favorable impact in the modernization. The information security concept in the computer networks is dealt with utmost importance and we need to create appropriate security measures and strategies in the current information security demand environment. The users of the networking devices such as Mobile phones, PC's or Laptops should be proactive and implement strategies such as firewall technology, encryption technology, network access control technology, and network virus prevention technology to successfully prevent these information security problems. This paper examines the security issues that arise in the use of wireless sensor networks and investigates the mechanisms for defending information security considering improving the security and stability of the wireless sensor networks through standard optimization and simulation techniques. The terms Wireless Sensor Networks or WSN's are interchangeably used throughout this paper.**

***Keywords**— Wireless Sensor Networks, Information Security, Data Privacy, Wireless Transmission, Local Area Network (LAN), Network Access, Wireless Fidelity (Wi-Fi), User Datagram, Intrusion Detection System (IDS), Virtual Private Network (VPN), Data Module, Reception Data.*

I. INTRODUCTION

The steady and continuous development of the computer and the wireless communication technology has given birth to many modern-day applications such as Wireless Sensor Networking technology, which are being steadily using in the Military warfare, Satellite Communications, environment monitoring and many other major applications. "This type of micro sensor network with computing and communication capabilities is a multi-hop self-organizing network formed by a large number of inexpensive micro sensor nodes connected by wireless communication, which can cooperatively complete data collection, transmission, and fusion of various monitoring objects in the deployment area" [1]. The latest technologies such as Wireless Sensor technology, computer technology, Wireless communication technology, and Distributed Systems technology have all been advanced in recent years, yielding in the enhancement and the performance of the wireless sensor networks. One of the major applications of the WSN is ensuring the data security and integrity in the military applications and spoofing the secure data from the enemy radars [2].

This application in the defence systems uses the concept of the Distributed Systems and Parallel processing technology which is flexible for the end-users of the artillery equipment. The rapid development in the Wireless technology has posed many challenges along with the benefits. Hence the study of the Security Issues and its prevention is the inevitable. Wireless Sensor Networks or WSN's are the networking sensors that collects and processes the data and is sent to the database in the central server location.

The sensor network is the independent unit typically with hundreds of small interconnecting nodes embedded in the large single network which aims to collect data, processing the received information datagram and retrieving at the regular intervals to maintain the synchronous full duplex communication rates [3]. The expansion of the networking technology has brought many challenges and the threats associated with the advancements has huge impact in security.

User Datagrams \\	WSN’s \\	Data Centres \\
Incoming Packets	Network Nodes	Central Location

Fig 1. Block Representation of Security Datagrams

II. Statistical Analysis of sensor networks

The network topology behaviour is unpredictable, and it changes from time to time. The values of the data will be different from before establishing the connection and after establishing [4]. The theory of establishing the network connection is connecting with each networking nodes before the start of the data transmission. The wireless transmission of data is vulnerable to many threats at the physical and data link layer. Despite the widespread adoption of the computer network, some computer users are unaware of network security and do not pay attention to the installation and updating of anti-virus software and firewall systems, exposing personal information and jeopardizing network security [5]. The final phase in the network operating process is data transmission. At this level, malicious destruction will result in tampering and the loss of all transmitted data. The Internet architecture conceptual model is hierarchical.

It is required to perform security work in the present computer network operation process. Starting with the existing state of computer network security, we should take appropriate safeguards to assure the absolute security of network data [6]. When a virus infects a computer system, it can copy and destroy essential data and applications, rendering the network inoperable and causing the system to crash, resulting in significant financial losses.

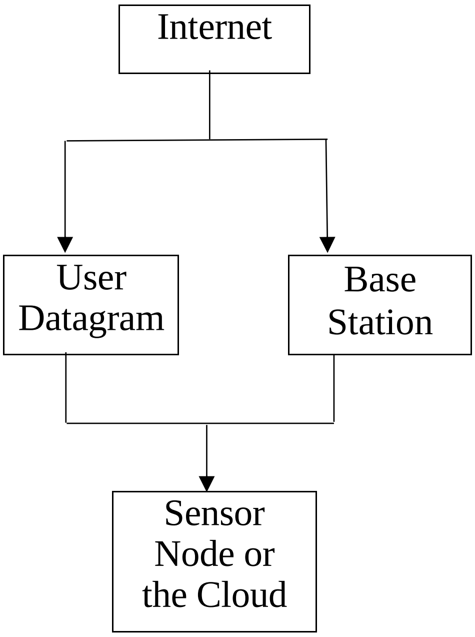

Fig 2. Wireless Sensor Network Topology

Advanced equipment can be used in the actual attack process to send data packets to the wireless sensor network on a regular basis, effectively blocking communication within the wireless sensor network, or advanced equipment can be disguised as a base station to monitor the wireless sensor network. Both endpoints of the data transfer are aware that the key used to decrypt data files is symmetric. The lightweight encryption approach can lessen the burden on sensor nodes in the real world. As a result, when data encryption is performed, this type of technique is typically employed [1]. When an information security incident happens because of unforeseen circumstances, the problem can only be rectified to a large extent by artificial maintenance and management. The graphical representation in the Fig. 3 shows the analysis of the WSN’s deployment over the years and the dependency on the wireless network has increased exponentially.

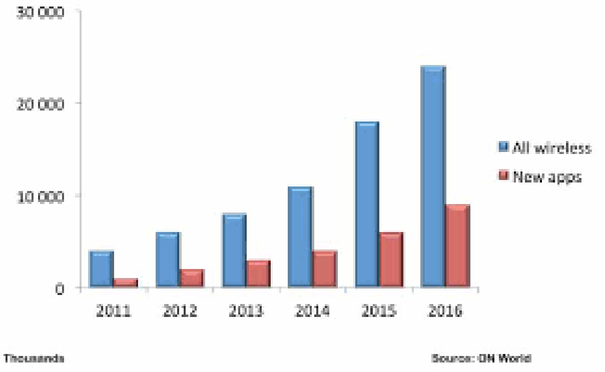

Fig 3. Analysis of WSN’s deployment

Network security refers to the protection of the network system's software and hardware, as well as the data contained inside it, from accidental or malicious damage, modification, or leakage. In this method, most typical network hacker problems occur; they will consciously filter and intercept network data, and after illegally infiltrating the computer, personal privacy information will be stolen as well. Computer network virus is a term used to describe a viral software that enters a normal computer network system and causes damage to the computer system and network [7]. Wireless communication is easier to monitor than traditional wired networks. The preceding data packets can be easily replayed by introducing a bit stream. However, there is usually no technical team involved in the setup of wireless sensor networks, and once the equipment is installed, it is entirely dependent on the equipment to function. The acquisition of network nodes is a breeze with this manner of operation [8]. After locating the matching nodes, the attacker can either replace them with additional sensors or change the memory to monitor the entire wireless sensor network. When a computer network's security is compromised, it is very likely to result in unfathomable losses and repercussions.

III. Optimization technques

The increasing importance and securing the network system has always been a top priority. The technologies presented in this paper are Network Access Technology and the Network Virus Prevention Technology with some of the enhanced features [9] present in the wireless sensor networks.

A. *Network Access Control Technology with IDS*

The optimization techniques presented is viewed as the countermeasures for data prevention using wireless sensor networks. The NACT is enhanced with the IDS in this research paper [2]. Accordingly, from the computer network managers standpoint, the improvement is solely dependent on the local area network management, correct our work attitudes, improve the network security management process, create a good computer network operating environment [3], and realize effective professional and technical level promotion. Network access control technology is frequently utilized in the prevention and protection of network security. It is separated into four categories: network access control, network authority control, network server security control, and attribute security control, which can effectively prevent network resources from being utilized or accessed in a prohibited manner.

The acquired information can be easily converted into the assembly file format using the assembly software, allowing confidential information such as programme code, routing protocol, and key stored in the sensor node to be analysed while the programme code is also modified and loaded into the sensor node. To strengthen the security of computer network systems, computer network users should constantly improve their own security awareness, select relatively complex login passwords, encrypt files in computer systems, and correct defects on a regular basis [10].

Majority of the attacks on the wireless sensor networks happens in the network layer, for example, by altering routing information, impersonating the network route, and attacking sequence followed by spoofing in the wireless sensor network will directly invade the network or cause the original route to generate incorrect data sequence. The IDS representation [8] of NACT technology is shown in the figure below.

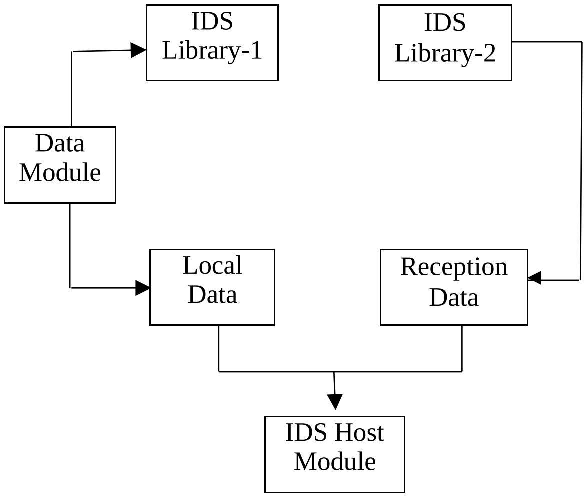

Fig. 4. NACT with IDS Representation

B. *Network Virus Prevention Technology*

The configuration using the network firewall will aid us in assisting foreign user access and attacks, enhancing the computer network security avoiding the potential security hazards and efficiently controlling the network management behavior. The basic goal of network virus protection technology is to put up some complete virus prevention software, ensuring that the software can be automatically upgraded, and that appropriate instructions can be automatically popped up in operation to avoid viral invasion [5]. The primary aim of sensor networks is to collect data. Eavesdropping and connecting fake unauthorized nodes are two ways for attackers to access sensitive information. If the attacker understands the relevant algorithm for extracting restricted information from multi-channel data, he or she can derive useful information from a significant amount of data. After a LAN connection, it is vital for enterprise computer systems to not only resist and avoid trojan viruses and system vulnerabilities, but also to increase the prevention of "hacker" attacks [7]. It is vital to have a management level to manage everyday work and an implementation and maintenance level to be accountable for the implementation of safety plans and decisions to implement the decisions of the decision-making level. The information security organization is structured in a hierarchical manner. The human aspect is also highly significant in the critical link of network information system security. Strengthening the capability and quality training of professional and technical team, as well as popularizing information security knowledge among business system users, can help to make computer and network equipment more secure, stable, cost-effective, and reliable [7]. Anti-virus software should be implemented in the computer network system to detect and eliminate viruses that have infiltrated the system [10]. If you can't check and kill the virus, you'll need to update your viral library. If the infection cannot be checked and killed, it should be uploaded to an anti-virus website for assistance.

IV. SIMULATION TECHNIQUES

To efficiently analyse the data parameters in the WSN’s, the set of values are passed as the input to each interconnecting node of the wireless sensor networks. This process is followed for one set of interconnecting nodes and repeated on various interconnecting nodes in a huge wireless sensor network grid. The nodes are placed as the 802.11 configuration locally.

A. *Network Simulator 2.0*

Network simulator 2.0 or the GNS 2.0 is the software simulation tool that exactly has the same rich features of the real network. This process is achieved by simulating or interactions between various network parameters such as routers, switches, inter-connecting nodes, access points and links. Most of the simulators utilize statistical event simulation for the system modelling with which the parameters are varied depending on the statistical simulations. The various attributes relating to the network entities and the devices of the tool environment can be modified and labelled in a controlled manner based on the network protocols in the tool libraries under different condition. The NS or Network Simulator version 2.0 is an upgraded software tool, that has enhanced features of duplex communications.

B. *Simulation Results for the WSN using GNS or NS 2.0*

The interconnecting nodes are treated as the access points present in the tool libraries. The datagrams sent from one access point reach to the other access points with multiple hops throughout the network layer. The vulnerabilities are detected with discrete time modelling at each access points and marked at t = 0. The packet from the first node reaches the second interconnecting node at time t =1 when there is no intrusion while traversing.

At t = n, the packet will reach the final interconnecting node and the percentage of IDS alerts are rolled out in the Real-Time (RT) tab. The results include an analysis of the network device metrics and their performance for each IDS alert.

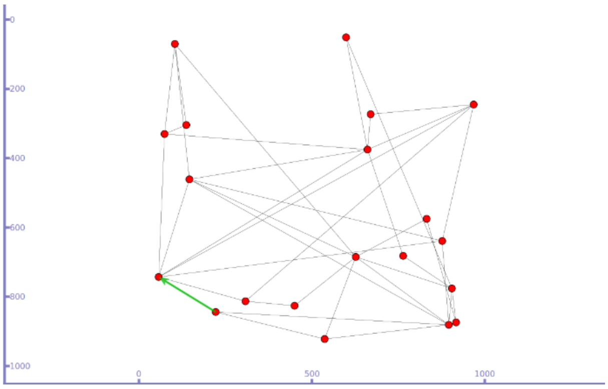

Fig 5. Discrete Event Network Simulator 2.0

V. APPLICATIONS

Generally, information security is employed in government sectors, financial services, manufacturing businesses, software & internet services, retail & wholesale lines, and healthcare industry. As it provides, cutting-edge critical benefits like 24/7 protection, increase service uptime (protect from time-consuming & expensive disruptions & outages), reduce attack surface (eliminate complexity, patch vulnerabilities, & secure network entry points to reduce cyber risk), guarantees visibility (quickly identify threats & anomalies with real-time monitoring across the entire network environments), helps identify gaps(assess how the landscape of ICS, OT, and IIOT systems interact with primary networks and systems to minimize risks), safeguard IP and customer data with the latest security solutions, controls, and policies.

Furthermore, it toughens security posture (embed security in business models from device to server to cloud), secure digital assets, block advanced threats national-state attacks, secure end-user, boost security maturity. Thereby, achieving long-term compliance, identifying security weakness, accurately access risk.

VI. FUTURE RESEARCH, SCOPE & ENHANCEMENTS

Based on my evaluation and investigation, I have suggested the simulation technique using network simulator tools like GNS2. Additionally, we could use GNS3, Putty or WIRESHARK tools & software’s for advanced security and safety. Similarly, various other information security technologies that can be used are authentication of hardware, user-behavior analytics, tokenization, deep learning, and data loss prevention technique. Also, IPS (Intrusion Prevention System) and SIEM (Security Incident and Event Management) can be used.

VII. CONCLUSION

It is vital to raise users' security awareness and face up to the challenges that exist in the operation of computer networks, as well as to design efficient preventive measures, reinforce computer system maintenance and detection, and update anti-virus software on a regular basis. Wireless sensor networks are becoming increasingly widespread. We must actively research the security defence mechanism with a professional attitude to address potential security issues, and we cannot deny the relevance of the existence of wireless sensor networks due to current issues. Currently, improving and optimizing computer network information security procedures is a critical component of computer network security.

We should combine the requirements for computer network security, make targeted changes and upgrades, and choose and implement technology wisely. Information security in computer networks is extremely complicated, and there are numerous influencing elements. According to the contributing factors, preventive steps should be taken. Data encryption technology can safeguard the dynamic information of a computer system in real time, which can not only prevent passive attacks and improve the security of the computer system, but also intercept the invasion and attack of other programmes in the first place. We can only boost the development of productive forces and the progress of information technology by grasping the science and technology development trend and working to minimize the development's disadvantages.

VIII. ACKNOWLEDGEMENT

This research analysis paper is developed for Prof. Luke Russell in partial fulfilment for the requirements for the course SYSC-5902 Research Methods for Engineers Fall-2021. I would like to thank the professor for the opportunity and support for the research.

IX. DECLARATION

I hereby declare that this research analysis paper is presented based on the knowledge from other research papers, seminars, journal proceedings, and the technical reports. The facts and the figures are used for representational purpose of the data, and the simulator tool attributes are furnished from the authentic sources of the IEEE reports based on wireless sensor networks datasheets.

X. REFERENCES

[1] Haiwei Wu, Hanling Wu “*Research on Computer Network Information Security Problems and Prevention Based on Wireless Sensor Network* ” IEEE Asia Pacific Conference on Image Processing, Electronics and Computer, 2021, pp 1015-1018

[2] Carl E Landwehr, David M Goldschlag “*Security Issues in Network with Internet Access*”, Proceedings of IEEE,Vol 85, No 12, USA 1997, pp. 2034 – 2051.

[3] Yiming Huo, Wei Xu “*Cellular and Wi-Fi Co-Design for 5G User Equipment*” University of South California, USA 2018, pp. 256-261.

[4] Fan Yan, Yang Jiang-wen, Cheng Lin “*Computer Network Security and Technology Research*” 2015 Seventh International Conference on Measuring Technology and Mechatronics Automation, China, 2015, pp. 293-296

[5] Albandari Mishal Alotaibi, Bedour Fahad Alrashidi, Samina Naz and Zahida Parveen *“Security Issues in Protocols of TCP/IP model at Layers Level”* International Journal of Computer Networks and Communication Security, Saudi Arabia, May 2017, pp 96-104.

[6] Roumen Trifonov, Georgi Tsochev, Galya Pavlova, Radoslav Yoshinov, Slavcho Manolov “*Adaptive Optimization Techniques for Intelligent Network Security*” Fourth International Conference on Mathematics and Computers in Science and Industry, Sofia, 2017, pp 219-223.

[7] Michael Kuhl, Jason Kistner, Kevin Constantini, Moises Sudit "*Cyber Attack Modelling and Simulation for Network Security Analysis*" IEEE Proceedings of the Winter Simulation Conference, New York, 2007, pp 1180-1188.

[8] Jujinquan, Mohd Abdulhakim and Ahmad Abdulhakim "*Analysis and Protection of Computer Network Security Issues*" Internation Conference on Advanced Computer Network Technology, ICACT, pp 577-580.

[9] Charles Ellis, Quishi Wu "*A Game Theory on Network Security*", Proceedings of the 43rd Hawaii International Conference on System Science, pp 1-10

[10] Qingdong Meng, Danli "*Research and Application based on Network Security Monitoring Platform and Device*" 2019 IEEE PES Innovation and Smart Grid Technology Asia, pp 716-719.

[11] Shailajay Pandey "*Modern Network Security: Issues and Challenges*", International Journal of Engineering Science and Technology, Vol 3, pp 4351-4357.

[12] Hadi Shiravi, Ali Shiravi, A Ghorbani, "*A survey of Visualizations of Network Security*", IEEE Transactions on Visualizations and Computer Graphics, Vol 18, 2012, pp 1039-1046.

[13] Mohav V Pawar, Anuradha J, "*Network Security and Types of Attack in Networks*", International Conference on Intelligent Computing, Communication and Convergence, 2015, pp 506-5012.

[14] Tadashi OHTA and Tetsuya Chikaraishi "*Network Security Model*", ATR Systems and Laboratories, Kyoto, Japan, pp 209-215.