A survey paper on packet data security

Ritika Gupta[1] & Alok Srivastava[2]
[1]M.Tech Student, Department of ECE, Chadrawati Group of Institution

Received: September 21, 2018 Accepted: October 31, 2018

ABSTRACT: *Now a day's majority of data exchange between source nodes to destination node is performed through wireless network with higher order of data privacy, data integrity, data authenticity and data freshness. Data privacy is a ensuring that all packets on the network are inaccessible by the hackers and data integrity is ensures correct data is received. But in such a modern time threats to break the security of network is increases day by day, so the network security is always a challenge field to protect the data lost during transmission session. This paper includes packet data security and their issues, various network attacks for accessing the data and also a comparative study of different security techniques for data transmission between to end users without any data lost.*

Key Words: *Packet data security, wireless Attacks, data security topologies, wireless sensor network.*

1.0 Introduction— In such a modern day's there is no expectation to live a good life without computers and the Internet; they both are correlated to each other not inseparable. Both are used to connect the any computer with the world and other one is used to transferring the lot of data through it. Data security means a process to block the unauthorized access of data to someone, when unauthorized access is enabling then it may create a lot of problem so data security so to protect the digital data from destructive forces and from the unwanted actions of unauthorized users, such as a cyber attack. A packet is just like a container that contains valuable information that can be transferred from one commuter to other through TCP/IP network or sub interconnected networks, so data security is the primary need in data transmission to the receiver without losing any information. Packet data security is a measure of to prevent the loss of data through unauthorized access. There are many ways to protect data, and some one of them includes strong user authentication, encryption, data erasure, backup etc. When someone need to secure data transmission, by the concept of packet data security, which involves the corrective action taken to Ease of Use protect from the viruses, hacking and unauthorized access of the data .

1.1 Main Cause for packet data loss

Packet data loss means when the destination point is not able to receive the correct information during their transmission through a channel. There are many reasons behind data loss but commons are

(a) Network Congestion: when network become more congested due to traffic or hit maximum capacity to handle the data by a network. In that case the packet is waiting for your turn to be delivered in between if connection is fall the data is discarded and valuable information of packet is lost.

(b) **Software Bugs:** when at the time of data is transmission through a network, software bugs is created then transmitted data is lost because the bugs is automatically resolved by the rebooting the system.

(c) **Problems with Network hardware:** Due to outdated network hardware like as routers, network switches, firewalls can slow down the traffic, so the data is waiting for your turn and in between some data is lost due to time out.

1.2 Need of data Security

In data transmission system the valuable data is transferred from source to destination through medium or TCP/IP network and interconnected sub networks. So there are more and more chances for losing the data due to hardware parameter and threats issues. There are few main reasons to protect the data when it transmitted through networks are;

(a) Data Confidentiality: It is an assurance that an authorized user accesses the information. It is the most challenging task in network security because the radio spectrum is open to all, so there is more chances an attacker can spy the transmitted packet through air.

(b) **Data Authenticity:** It is a process to identify the communicating node. In data transmission it is very important to identify the sender node because to identify that received data is received from correct node or not.

(c) **Data Integrity:** Due to channel fading, time-frequency coherence, inter band interference and operating condition like as change in temperature & humidity, may cause errors in packets and these error packets are transferred to forward node without any prior information to receiver node. So data integrity is a ensure that the received data is not changed during transmission channel due to malicious intent.

(d) **Data Freshness:** Data freshness is basically used to ensure that no old message or data replayed so to ensure freshness of the packet a timestamp is attached with packet and receiving node compare this timestamp in the packet with own clock and determine wheatear the received data is fresh or not.

(e) **Data Availability:** Due to large excess of computation, sensor node become out of power i.e. unavailable, so at that time attackers may jam the communication network and spy the transmitted data. Availability is ensuring of ability to provide expected services for which they are designed.[3]

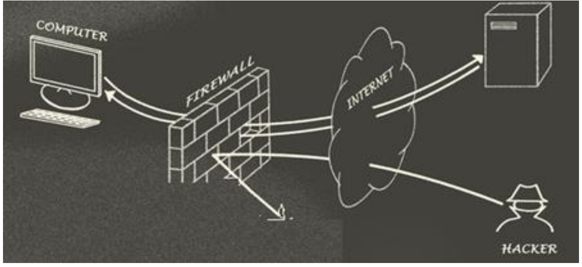


Fig: 1 Basic block diagram for data Transmission

1.3 Various Attacks in wireless network

The Attacks are used to access the information inside the packet. There are some main attacks discussed below.

(a) **Traffic Attacks**: In this attack the attackers are able to take over the packets during their transmission session

(b) **Passive Eavesdropping**: In the attack the attackers are able to watch over the unlimited wireless session on data packet.

(c) **Active Eavesdropping**: In the attack the attackers are able to watch over the data packet and actively insert your message during wireless transmission session.

(d) **Man-in-middle attacks**: In the attack the attackers are able to read the data during wireless session.

(e) **Hijacking**: In this attacks the owner is knows that there is no access of data but actually the hackers used it.

(f) **Jamming Attack**: This type of attack is used by the hackers to Jam the traffic network so they easily modify the data of get the valuable information

1.4 Data security topologies

For data securities there are different topologies are

(a) Disk Encryption
(b) Backups
(c) Data Masking
(d) Data Erasing
(e) Software v/s Hardware Mechanism

Disk Encryption is a technology which is used to protect the data by converting it into unreadable form that cannot be opened easily by unauthorized users. In disk encryption with the help of disk encryption software data is encrypted bit by bit. It is also used to block the unauthorized access to data storage.

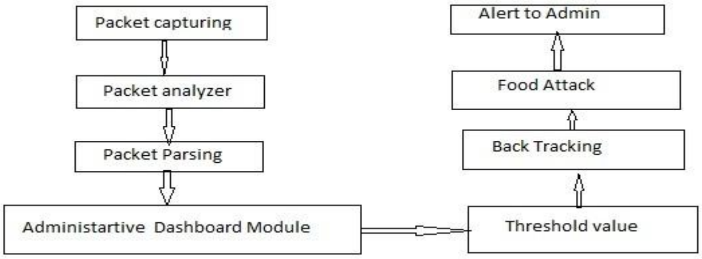
A backup is a technology in which information data is backing up or copying the data files into an archive file of the computer. The primary purpose of data backup technology is used to restore the original data after when the data is lost due to corruption and secondary one is to restore the data from an earlier time according to a user defined data retention policy.

Data Masking is process in which specific data within a database table or cell to ensure that the sensitive information regarding original data is not exposed to unauthorized users.

Data erasure is a software based method to protect the data from unauthorized users. In this technique information data is completely overwrited with the help of software, so no sensitive data is lost when an asset is retired or reused.

In software versus hardware based mechanisms the original data files are corrupted or overwrited with the help of software to make it in unrecoverable form or making the system unusable form.

Basic block diagram of packet security system:



2. Review of Literature

Sneha Vinod Kumar et al (2017) proposed an algorithm for packet data security based on the attack time and also inform the administrative bodies regarding security issues. In this method first of all the transmission network is monitored and after that the data [packet is captured then captured data packet the extracted, parsed and then based on the duration of attack time, an alert is made to the main bodies or systems.[1]

Aditya Sharma et al (2015) presented a survey on various issues in wireless sensor network along with types of security issues in wireless sensor networks. In the paper various types of security issue like data integrity, confidentiality, authentication etc. Writers also discussed various protocols already implemented and proposed. [2]

S.K Singh et al (2015) presented a survey on wireless network security issue. According to the paper security has become a major issue in wireless security issue. It has also discussed various issues of low energy in wireless sensor network. It has also given emphasis on low overhead for data security protocols.[3]

Agustinus Jacobus and Alicia A.E. Sinusw (2015) proposed an intrusion detection system using a data mining techniques to detect the pattern online. In the existing intrusion detection system in computer network also apart of network security that is used to detect the intrusion action before it makes more damage but by increasing the no. of internet activity this system not able to provide better efficiency. So with the help of this data mining techniques intrusion are easily detected only before creating more damage or data lost. [4]

G.S. Mamatha and S.C. Sharma (2010) give a comparative study for network security and also focus on Mobile ad hoc network and different types of network layer with how to protect form the attacks when the data transmitted from source to destination node. There is a main security issues in mobile ad hoc networks to protect the network layers from serious attacks. So it is necessary to identify the route data forwarding operations in network layers. Due to undetectable malicious node then this node is easily read with route function that makes lot of damage in data packets. In this paper author is also give a study of MANETs attacks on route nodes and how it is handled. [5]

According to shailja pandey (2011) network security is basic need for data transmission through a network for any organization without any data lost or more secure data packet transmission. Now a day security threats are increases very fast day by day and due to wireless transmission and internet services it become more insecure because the data packets are transmitted through air so any one attacks on the data packet by just tracking the transmission frequency band spectrum and easily access the valuable information. In his paper author discuss the different techniques for data packet security and network security without losing the data. [6]

According to Raju Ramaswamy for an efficient and more secure voice communication system first of all the voice packet are to be encrypted at the source or end-user node and then transmitted through a wireless medium to destination node. At the destination node the received packet is decrypted in order to form an original voice signal. In his paper discussed the voice communication system with secure data transmission using DES (Data Encryption Standard) and Public Key cryptographic algorithms. When the signal is encrypted at end user node there is some problems are encountered like as voice packetization delay, voice packet encryption/decryption delay due to symmetric/asymmetric Cryptographic algorithm, proper selection of node, error control and flow control issues and session key generation and distribution issues for encryption/decryption.[7]

Manolis Sifalakis et al (2005) Proposed a mechanism based on Network Address Hopping to reduce the communication delay between source node and destination node with highly secured network without losing a packet data. He develop a NAH (Network Address Hopping) based mechanism, when the data is spread over a more than one end users and stop the exchange of data between source and destination by shuffling the communication pattern. With the help of developed novel technique the user is able to proactive protection against Interception, Anti Jamming protection and Complement existing security by adding redundancy and diversity. [8]

On the basis of literature review Surjit Paul and sanjay Kumar (2016) proposed a comparative study for data Security of different wireless networks (WPAN, WMAN & WWAN) with their merits and demerits. According to the author WLAN and WPA2 are the efficient security networks for data transmission through wireless network.[9]

4. Conclusion

Now a day's data packet security become most important parameters for big organizations because each organization share your valuable information through a wireless network when the data is transferred through wireless network then there is more chances to access the valuable information of the data packets by the hackers just by tracking the data transmission spectrum. So on the basis of literature review there are many protocols or security threats for wireless transmission like SPINS (Security protocol for sensor network), SNEP (for good confidentially and message authentication), TINYSEC (Tiny Sec in link layer security), LEAP (Localized Encryption and authentication protocol) etc. In this paper some we introduce the basic idea about data security, main reasons behind insecurity and some basic data security topologies when they are implemented then very fruitful for secure data transmission.

5. REFERENCES:

[1] Sneha Vinod Kumar, Yashashwini V, Anusha Pai G, and Dr.Yuvaraju B.N, "Security of the Network Based on Duration of Attack," Int'l research Journal of Engineering and Technology (IRJET), vol. 04, no. 4, pp. 2315-2318, April 2017.

[2] A. Sharma, G. Tripathi, Mohd. S. Kahan, and K. Anil Kumar, "A Survey on Security Protocols of Wireless Sensor Networks," Int'l research Journal of Engineering and Technology (IRJET), vol. 02, no. 08, pp. 1548-1552, Nov 2015.

[3] S.K. Singh, M.P. Singh, and D.K. Singh, "A Survey on Network Security and Attack Defense Mechanisms for wireless sensor network," Int'l Journal of computer trends and Technology, pp. 2231-2803, May-June 2011.

[4] Agustinus Jacobus and Alicia A.E. Sinusw, "Network Packet Data online Processing for Intrusion Detection System," in Proc. IEEE Int'l Conf. on Information and Automation (ICIA), 2015.

[5] G.S. Mamatha and S.C. Sharma, "Network Layer Attacks and Defense Mechanisms in MANETS- a Survey," Int'l Journal of Computer Applications (0975 – 8887) vol. 09, pp.09, November 2010.

[6] Shailja pandey, "Modern Network security: issues and challenges," Int'l research Journal of Engineering and Technology (IRJET), vol. 03, no. 5, pp. 4351-4352, May 2011

[7] Raju Ramaswamy, "Design of a secure packet voice communication system in wide area networks," in IEEE on Network 1(2):6-10, pp. 43-50 April 1987.

[8] M. Sifalakis, S. Schmid, and D. Hutchison, "Network Address Hopping: A mechanism to Enhance Data Protection for Packet Communication, "Design of a secure packet voice communication system in wide area networks," in IEEE Int'l Conf. on communication, pp. 1518-1523, 2005.

[9] Surjit Paul and Sanjay Kumar, "A survey on wireless security," Int'l research Journal of Engineering and Technology (IRJET), vol. 03, no. 11, pp. 396-410, December 2016

[10] G. Ambika and P. Srivaramangai, "A Study on Data Security in Internet of Things," Int'l Journal of computer trends and Technology, vol. 05, no. 02, pp. 464-469, March-April 2017

[11] Abdel-Karim R. Al Tamimi, "Security in Wireless Data Networks: A Survey Paper," Int'l Journal of computer trends and Technology, Apr 23, 2006.

[12] Sandra Kay Miller, "Facing the Challenge of Wireless Security," July 2001.

[13] T. Kiravuo, M. Sarela, and J. Manner, "A Survey of Ethernet LAN Security," in IEEE Communications surveys & tutorials, 2013.

[14] Jose Perez, "A survey of wireless network security protocols," Int'l Journal of Computer Applications, 2005.

[15] Gurkas G.Z., Zaim A.H., and Aydin M.A., "Security Mechanisms and their Performance Impacts on Wireless Local Area Networks, 2006 International Symposium, vol. 01, no.05, pp.16-18 June 2006.