ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 8, February 2016

# Content Security Using Data Aggregation Technique in Wireless Sensor Network

Hannan Ansari, Tabrez Khan, Wasim Khan,
Department of Computer Application, Integral University, Lucknow, U.P, India

***Abstract*— *Wireless Sensor Networks are also a type of Network having a small and large number of sensor nodes with limited sensing computation and communication capabilities. Basically Wireless Sensor Networks are nothing but a type of network which has some sensing devices with communication capabilities. It has some advantages and disadvantages according to their use in different fields. To increase the life time of network, it is necessary to reduce the number of bits transmitted over the channel; if it happens then automatically the life time of network will increase. The proposal of this paper is to use a data aggregation method for reducing the data transmission over the network. There are a lot of security issues in data aggregation for example data integrity, confidentiality and freshness. So data aggregation becomes a crucial when the Wireless Sensor Network is deployed in remote environment or hostile environment where sensors are prone to node failure and compromises. Secure data aggregation schemes are fruitful to achieve the security in Wireless Sensor Networks. In this paper, the proposed secure data aggregation schemes provide end to end data privacy. Through this technique the average number of bits transmitted per node is reduced by 35%-50%.***

***Index Terms*— Network Security, Software Engineering, Cryptography, end-to-end privacy, Data Structure, Wireless Sensor Networks;**

## I. INTRODUCTION

Wireless Sensor Networks has become popular network due to its unique attributes such as their light weight, low coast, small memory size, limited power and energies supply, and ad hoc nature. However WSNs is vulnerable to may attacks and the security can be affected by these attacks. WSNs have some problems like limited power, unreliable communication (e.g. unreliable transfer, conflict and latency) and unattended operation. So Researchers have started focusing on building a model that's name is "Sensor Trust Model" (STM) to solve these problems. And they have tried to resolve the challenges of maximizing the processing capabilities and energy reverse of wireless sensor nodes and also securing them against Viruses, Worms, hackers, and some malicious activities. Wireless Sensor networks and electronic enabled the development of low cost, low power, and multifunctional sensors nodes. These small sensor nodes consisting of sensing, data processing and communication components, and these attributes make it possible to deploy wireless sensor networks, which show some improvement over the traditional wireless sensor networks. [1]

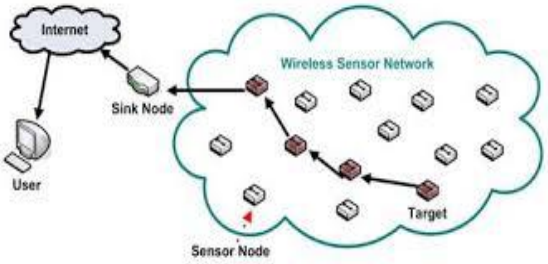

**Fig-1. Accessing Information by user in WSNs Mode**

### *A. Security Parameters*

According to network security, these terms are played major role to protect the given network and its entity like: Hosts, Communication Channel, Information presented at Senders and receivers sides.

**1. Cryptography:** In Computer science Cryptography is a art and technique to hide data in the form of cipher text. **"The many schemes used for encryption constitute the area of study know is cryptography".** It provides security to secure the plain text converting into cipher text with the help of different-different encryption techniques.

**2. Plain Text:** It is an original message, it means readable message is known as plain text. For example: "Rawan was killed by Great Rama in his kingdom that name is LANKA". here this sentence has a meaning, you can easily understand after reading this sentence.

**3. Cipher Text:** It is the converted part of original message, it means non-readable message is known as cipher text. For example: "#@#78@#!67(){}.///,\}\{=***^%$#@!~`". here this sentence is meaningless, you can't understand after reading this sentence.

**4. Encryption:** The process of converting from readable message to non-readable message is known as encryption technique.

**5. Decryption:** The process of converting from non-readable to readable message is known as decryption technique.

### *B. Data*

The term content or data or information is very important thing for network, without content we can't imagine about data communication over the network. So it is important aspect for data communication. In computer network the content presents in the form of data raw data. [1]

## II. PROBLEM DEFINITION

In the field of Network Processing techniques such as sensor data aggregation are used to reduce the communication overhead in wireless sensor Networks [2].

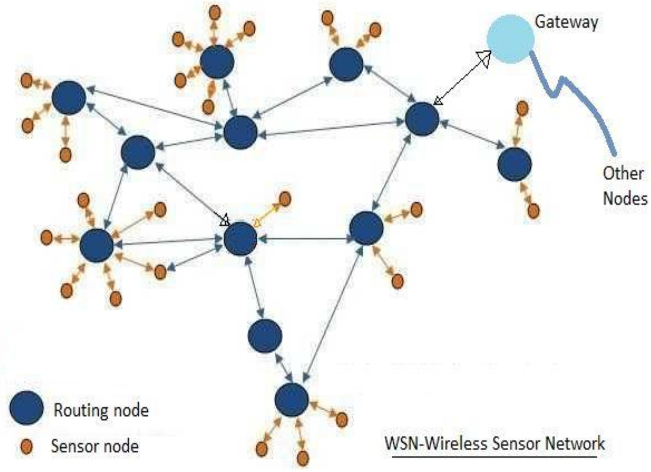

**Fig: 2, The Working Concept of Wireless Sensor Network**

Such type of technique refers to use an function f, that refers to aggregation function such as SUM, AVG, MIN, MAX, MULT etc. Suppose there are n data items, at intermediate nodes, it produces one aggregation value, which is equal to:

$$\mathbf{v = f( x_1, x_2, x_3 \ldots\ldots\ldots, x_n )} \qquad \text{----} \ (1)$$

Where:

v = aggregation value

f = aggregation function

and $x_1, x_2, x_3 \ldots\ldots, x_n$ = data items

The benefits of aggregation data on intermediate nodes are:

I. It reduces the energy consumption

II. It minimizes end to end delay and also bandwidth usage as well as improves the resultant of the network.

When proliferation increases in our daily lives of wireless sensors, It means the need of privacy and data aggregation automatically increase. In this research paper we are trying to address the issues of privacy and integrity of wireless sensor network. [2] According to privacy, data privacy and it pertains to hide the details of a nodes data from other one in the given network. The privacy term can be achieved by the technique encryption. Integrity: An unauthorized users can't modify the sensitive data or information of nodes, it provides prevention. Integrity can be achieved by the technique peer monitoring, which doesn't work with randomize data. [3][2][1]

Suppose we are considering that a WSN is an collection of n nodes, organizing in a tree hierarchy and rooted at the Base Station as given above Figure-2. [2] Privacy is always based on well known concept of semantic security. An adversary can not find out any information about the plaintext from its cipher text in the time of polynomial.

## III. CONTENT PRIVACY OVER NETWORK

"The field of Network and Internet Security" consists of measures to deter, prevent, detect, and correct security violations that involve the transmission of information". The definition introduces three key objectives that are at the heart of computer security:

- Confidentiality
- Integrity
- Availability and these three concepts form what is often referred to as the CIA?

**A. Confidentiality:** To be secured, information needs to be hidden from unauthorized access.

**B. Integrity:** Protect from unauthorized changed.

**C. Availability:** Available to an authorized entity when it is needed.

## IV. IP SECURITY

**IP Sec** provides the capability to secure communication across a LAN, across private and Public WANs and across the Internet.

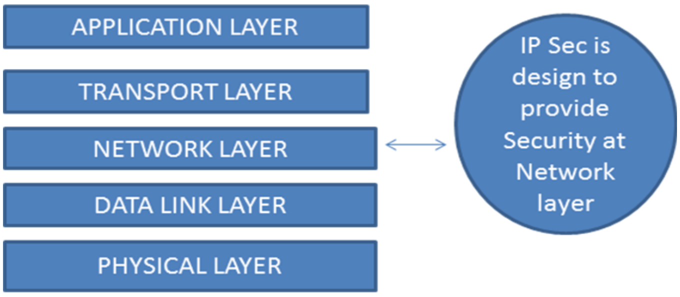

**Fig: 3. IP Sec Protocol**

Within the LAN, We identify System through IP address and within the System or hosts we identify the application with the help of port number. if we apply security at Transport layer then a particular application will secure.

**Network Layer:** When we talk about the network layer security it means we will talk about "router security" between two hosts. When we apply security at Transport layer with App1 and App3, It means App1 and App3 will be secured but App2 and App3 will not be secured as mentioned given bellow figure: 4.

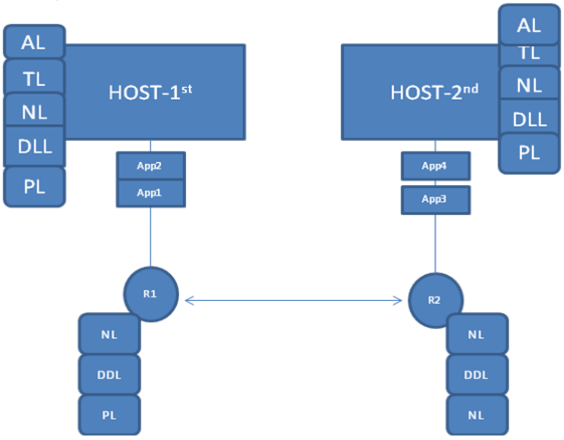

**Fig: 4. Router Security on Network Layer**

According to this security problems IP Sec applied two types of security:

- Transport Mode
- Tunnel Mode

***Transport Mode***

In Transport Mode IP Sec protocols deliver the packets from Transport Layer to Network Layer. In Transport mode IP Sec doesn't protect the IP header, it only protects the information which comes from Transport Layer.

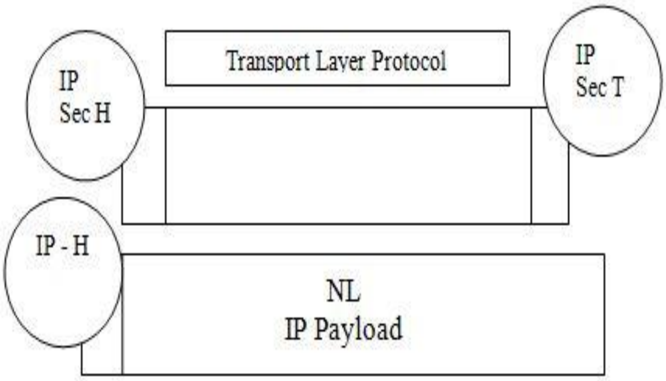

**Fig: 5. Adding header and tailer on Given Packet**

**Tunnel Mode:** In Tunnel Mode IP Sec protects the entire IP Packet. It Takes an IP Packet, including the header, applies IP Security methods to the entire packet and then adds a new IP Header, according to Figure: 5.

1. IP Sec in Tunnel mode protects the Original IP header.
2. Tunnel mode always established between
   - ✓ Router to Router
   - ✓ Router to Host

but transport mode always established between Host to Host. IP Sec defines two security protocols:

1. AH (Authentication Header)
2. ESP (Encapsulation Security Payload)

to provide authentication and/or encryption for packets at the IP level.

**AH**: The AH protocol provides source authentication and data integrity but not privacy. ( It is optional, now a days we are not using AH.). This protocol provides only authentication not encryption due to this reason it name is AH.

**ESP**: The ESP provides Source authentication, data integrity, and privacy. Now a days this protocols are using. The ESP protocol was designed after the AH, was already in use. ESP does whatever AH does with additional functionality (Privacy).

## V. AUDIT DATA GATHERING

Auditing is a new technique to collect information regarding the activity of users and applications. The OS is usually regarded as a trusted entity of a Host, because it is a resource manager, it controls access to resources, such as memory and files. Therefore several existing audit mechanisms are implemented within the OS. [1] OS audit data is not suitable for intrusion detection. Therefore in many cases, we see that the audit records produced by OS level auditing facilities, it contains irrelevant information and sometimes it provides lack of useful information. For the resultant, Intrusion Detection Systems has to access the OS directly to gather required data. [1][2] In past years, Several Researchers have worked on OS to identify what kind of information should be provided to "Intrusion Detection System" to be able to identify or detect intrusions effectively. For example, Lunt (1993) suggested the use of IDS-specific audit trails. Daniels and Spafford extended this initial idea and identified the audit data that OS needs to pro-vide to support the detection of attacks against the transmission control protocol/Internet protocol (TCP/IP) stack (1999). [1] The availability of OS level auditing technique always depends on the only operating System. Now some examples are given here: Sun's OS (first SunOS and later Solaris) provide some auditing information by Basic Security Module (BSM). The BSM is a type of Kernel extension that's allows one to log events at the system call level. The different auditing levels are specified and, in addition to system calls, security-relevant higher-level events can be generated as well (e.g., login events). Auditing is always disabled by the root user, and making such type of facility vulnerable to abuse by an intruder, hacker and attacker who gains administrative privileges on the Host side. [1][5]

**BSM** always produces audit records that are stored in audit files in a form of Binary format; the reason is that binary format always provides more space efficient. The main thing is that: the contents of an audit file will be available in human-readable format using The Praudit tool.

```
Thu Jan 10 23:01:29 2016 -> UID:root EUID:root RUID:root -
From machine:log1 execve() + /usr/bin/sparcv7/ps + cmdline:ps,-ef
+ success
Thu Jan 10 23:01:50 2016 -> UID:root EUID:root RUID:root -
From machine:log1 execve() + /usr/bin/tail +
cmdline:tail,/etc/system + success
Thu Jan 10 23:11:18 2016 -> UID:root EUID:root RUID:root -
From machine:log1 execve() + /usr/bin/pwd + cmdline:pwd +
success
Thu Jan 10 23:11:20 2016 -> UID:root EUID:root RUID:root -
From machine:log1 execve() + /usr/bin/ls + cmdline:ls,-l + success
Thu Jan 10 23:11:33 2016 -> UID:root EUID:root RUID:root -
From machine:log1 execve() + /usr/bin/ls + cmdline:ls,-l + success
```

**System Intrusion Analysis and Reporting Environment**: It wraps system calls in routines that gather the log information about process that always execute security relevant system calls. The other property of SNARE is it also supports simple pattern matching operations on the audit records produced, and these audit records can be used as a rudimentary form for Intrusion Detection. [5]

**Linux Intrusion Detection System**: LIDS, Ac-cording to its name, it is not an intrusion detection system but it also provides some additional features to its auditing capabilities. An access control layer that is complements and this access control layer always allow one to specify access for files, process and de-vices. [1][5][6]

## VI. CONCLUSION AND FUTURE SCOPE

According to Information World or Internet World, the term Data or Information plays an important role in Computer field. Without data we can't imagine about computer and related technologies. If data's privacy is not secure from unauthorized entity it's mean that we can lost data security. In Wireless Sensor Network it is a big problem in front client that how they will secure their data, information or content over the network. if an adversary achieve the sensitive data from the network, it means that he can play a big role in the given network. he can destroy the network, he can delete the data or he can modify the actual data sense. If he does then clients can be in great problem.

## SPECIAL THANK

I thanks specially to P**rofessor Syed Nadeem Akhtar (Ph.D)** the Director, Planning & Research Department, Integral University, Lucknow U.P, Who guided and provided us a lot of thought to elaborate the techniques and approaches of this research paper. I am glad that Sir given us lot of confident and amazing new born thought. I also thanks specially to **Prof Mohd. Faizan Farukhi (Ph.D)** the Head of Department of Computer Application of Integral University, Lucknow, U.P, Who guided and given us the sufficient time to focus on this research paper. Without his cooperation this research has not been completed in proper manner.

## REFERENCES

[1] Hannan Ansari, Sachin Kumar Patel, Sachida Nanda Barik. "Survey on Wireless Sensor Networks", International Journal of Engineering Development and Research (IJEDR), and ISSN: 2321-9939, Vol.3, Issue 1, and pp.266-271, Jan 2015, Available: http://www.ijedr.org/papers/IJEDR1501049.pdf.

[2] Kumar, Vipin, and Sanjay Madria. "PIP: Privacy and Integrity Preserving Data Aggregation in Wireless Sensor Networks." Reliable Distributed Systems (SRDS), 2013 IEEE 32nd International Symposium on. IEEE, 2013.

[3] Di Pietro, Roberto, et al. "Data security in unattended wireless sensor networks." Computers, IEEE Transactions on 58.11 (2009): 1500-1511.

[4] Boneh, Dan, and Matthew Franklin. "Identity-based encryption from the Weil pairing." SIAM Journal on Computing 32.3 (2003): 586-615.

[5] Hannan Ansari, Wasim Khan, Faizan Ahmad. "Secure Hosts Using Operating System Intrusion Detection In Wireless Sensor Networks." in INTERNATIONAL JOURNAL OF TECHNOLOGY ENHANCEMENTS AND EMERGING ENGINEERING RESEARCH, VOL 3, ISSUE 10 75 ISSN 2347-4289.

[6] Wasim Khan, Hannan Ansari, Anwar Ahamed Shaikh. "LOG FILES UTILITY FOR SOFTWARE MAINTENANCE." in International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 9, September 2015.

## AUTHOR BIOGRAPHY

**Hannan Ansari** completed B.E(IT) in 2012 and M.Tech in 2015 has experience in the area of IDSs, Software Engineering, Network Security, WSNs, Data Mining etc. He has total experience of more than 3 years in Software Industries in Web Development and Teaching and also published many Research Papers in various related fields currently working in department of Computer Application of Integral University Lucknow, U.P.

**Tabrez Khan** completed MCA in 2003 and M.Tech in 2010 has vast experience in the area of "Programming in C", Data Mining, Software Engineering, Data Structure etc, having experience of more than 12 years in teaching and also published many research paper in various fields, currently working as a Assistant Professor in department of Computer Application of Integral University Lucknow, U.P.

**Wasim Khan** completed B.Tech (IT) in 2006 and M.Tech in 2011 has vast experience in the area of "Big Data", Data Mining, IDSs, Software Engineering, Network Security, WSNs etc. He has experience of more than 9 years in teaching and also published many research paper in various fields, currently working as a Assistant Professor in department of Computer Application of Integral University Lucknow, U.P.