OPEN ACCESS

*International*
*Journal*
*Of Modern Engineering Research (IJMER)*

# Security and Adaptive Defense Mechanism in Wireless Sensor Networks

Anu John[1], Aswathi Prabhakaran[1], Abinaya[1], Prathima[1]
Pillutla Harikrishna[2*], R G Suresh Kumar[2]

*1 (Student, Department of Computer Science and Engineering, Rajiv Gandhi College of Engineering and Technology Pondicherry.)*
*2 (Assistant Professor, Department of Computer Science and Engineering, Rajiv Gandhi College of Engineering and Technology Pondicherry).*
**-Corresponding author- Email: pillutlaharikrishna@yahoo.co.in*

***ABSTRACT** : Security is the amount of resistance or safeguard from threats, this can be applied to many valuable asset. Security is the major concern for critical applications which are envisioned by wireless sensor networks (WSNs).These WSNs are vulnerable to malicious attacks and compromising them can have serious technical and economical problems. In this paper, we investigate the security related issues and challenges in wireless sensor networks. We also detect the various security threats and propose various security mechanisms for wireless sensor networks.*
***Keywords:** Wireless Sensor Networks (WSNs), Security, Threats*

## I. INTRODUCTION

Wireless sensor network (WSN) typically consists of a sink node which can also be referred as a base station which consists few numbers of wireless nodes. Sensor nodes have a low communication range, constrained battery power, computation power and storage space. The base station consists of unlimited available energy and is assumed to be secure. Those nodes are battery-operated devices with limited energy capacity and computational processing capability, requiring mechanisms to minimize their power consumption in replacement/recharging the battery. Wireless sensor networks (WSNs) have a wide range of applications such as battlefield surveillance, forest fire detection, traffic surveillance, flood detection etc. But wireless sensor networks are susceptible to a variety of potential attacks which obstructs the normal operation of the network. Several researches have been proposed on the security of WSNs. They can be divided into two categories: data security and infrastructure security. Data security considers how to design various key management schemes, encryption and decryption algorithms such that the data cannot be altered or integrated. Infrastructure security checks how to detect the attacks in the network. Further, the infrastructure security is also divided into two aspects: algorithmic security and system security. The idea of algorithmic security is to deploy redundant nodes so that packets can bypass the area under attack by being delivered through backup routers. The system security includes various mechanisms which includes WSN self-healing and immunity checking of the systems. Since the environment of sensor nodes is quit challenging, and it is impractical to manually manage nodes, people propose the idea of self-healing mechanism as this has the capability of self-recovery.

In this paper, we discuss the most common security service and defense mechanisms for WSNs. The paper is framed as follows. Section 2 focuses on security requirements. Section 3 explores various attacks in WSNs. In Section 4 seeks various security solutions. Finally, we conclude the chapter in Section 5.

## II. SECURITY REQUIREMENTS

Security in WSN is an important and vital requirement, as WSN are vulnerable against various security attacks. These attacks mainly occur due to the broadcast and wireless nature of the transmission medium. A sensor network shares some properties as the computer network as the sensor network is considered to be an Ad hoc network. Various requirements should be considered while designing of a security protocol which includes confidentiality, integrity and Authentication. The security requirements are classified as:

### 2.1 DATA CONFIDENTIALITY

Data confidentiality is one of major task in network security. Every network addressees this problem. Confidentiality is the guarantee that authorized person access the information. This ensures the protection of

sensitive information is not revealed to unauthorized third parties. Confidentiality is mainly known for privacy of communications, secure storage of data, granular access control and authenticated users. In WSN, the major requirement of confidentiality is that a sensor node should not reveal its data to its neighbor nodes. It is extremely important to build a secure channel in wireless sensor network as many applications communicate highly sensitive data. One of the standard approaches for achieving confidentiality is to encrypt the shared secret keys.

### 2.2. DATA INTEGRITY

In network security, data integrity means maintaining and assuring the accuracy and consistency of data. This means that data cannot be modified in an unauthorized or undetected manner. This mechanism ensures that messages cannot be altered or integrated when it travels from sender to receiver. The major aspect of data integrity is referential integrity. Referential integrity is the ability to maintain valid relationships between values in the database, according to rules that have been identified.

One of the major problems is caused when the attacker understands the packet format and the semantic meaning of the communication protocol. In this case, attacker modifies the packet content and sends it to the receiver so that the receiver can obtain the wrong information.

Data integrity is to ensure that information is not changed in transit, either due to malicious intent or accident. In this system and object privileges control access to application tables and system commands, so only authorized users can change the data.

### 2.3. DATA AVAILABILITY

A secure system makes data available to authorized users, without delay. But there are many approaches which limit the data access, or propose an unsuitable scheme. But these approaches weaken the sensor and the sensor network as additional computational and communication consumes more energy. And a single point failure will be introduced if using the central point scheme as this greatly threatens the availability of the network.

Denial-of-service attacks are attempts to block authorized users' ability to access and use the system when needed. A secure system must be designed in such a way to deliberate attacks, which might put it out of commission. And the performance would remain adequate regardless of the number of users or processing of demand of service. Availability can be referred as the information must be available when it is needed this means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channel used to access must function correctly.

### 2.4. DATA AUTHENTICATION

Authentication is a way of implementing decisions about whom to trust. This method seeks to guarantee the identity of system users. In information security, it is necessary to ensure that the data, transactions, communications or documents are genuine. It is important for authenticating to validate that both parties are involved whom they claim to be. Attacks in WSNs are not only caused due to the alteration of packets but are mainly caused due to the injection of fabricated packets in the network. The main idea of data authentication is to verify the sender.

Data authentication allows a receiver to verify that the data really is sent by the claimed sender. In a two-party communication, data authentication can be achieved through a purely symmetric mechanism; the sender and receiver share a secret key to compute the message authentication code (MAC) of all communicated data.

### 2.5. DATA FRESHNESS

For a secure wireless network, we should achieve data freshness of each message along with confidentiality, integrity and authentication. Data freshness ensures that data are recent and that no old messages have been replayed to protect data aggregation schemes. In WSN structures, sensors send measurement data related to environment in which they are present through specific time intervals. It is therefore important to check that the data is new. A counter can be added to the message packet or a random number can be used during encryption to maintain data freshness.

## III. Security Attacks in WSNS

Wireless Network Systems composed of a large number of sensor nodes which are typically deployed in hostile environments where they are encountered a large variety of malicious attacks. Sensor networks are vulnerability to a diversity of attacks on the different layers. The most important attack is denial of service attacks. Apart from this attack other attacks are privacy violation, traffic attack, Monitoring and eavesdropping,

physical attacks, node capture and so on. The most important challenging attacks on WSNs are Physical Layer DoS, Link Layer DoS, and Attacks on Transport Layer, Attacks on Routing, Sybil attack and Attacks on Data Aggregation

**3.1. Attacks in Physical Layer**

Physical layer is the one which is responsible for selection of frequency, generation of frequency, modulation, detection and data encryption. In WSNs nodes are fixed in a hostile environment in which the attacker can have the access. The attacks in physical layer are of two types which include: jamming and tampering.

**3.3.1 Jamming**

When the attacker consolidates with the radio iterations of WSNs, then jamming attack takes place. Jamming can be referred to as an attack interfering with the radio iterations when the nodes in the network are using jamming. In jamming attacks can be classified as Constant, Deceptive, Random and Reactive. In constant packets get corrupted while they are transmitted. In deceptive the attacker sends a fixed stream of data in the network to make it look like a natural traffic. And in reactive the attacker sends a jam signal when receives a sensation that the traffic has occurred. Typical defenses against jamming include variations of spread-spectrum communication such as frequency hopping and code spreading. Jamming is efficiently and well organized, a small number node that is attacking attenuates the whole network, yet the number of nodes in the network is greater than the number of attacking nodes. If the attacking node is positioned near to the gateway, then the node can immobilize the entire network. This technique restricts its use in WSNs due to the greater design complexity and energy.

**3.3.2 Tampering**

Tampering is a type of physical layer attack. If a physical access is given to a node, an attacker can take secret information like cryptographic keys or other data which can be used for future purpose. The node can be reformed or reintegrated to create a compromised node which could be controlled by the attacker. Tampering can cause a major physical damage. Various measures to control tampering involve self destruction and fault tolerant protocols.

**3.2 Attacks in Link Layer**

The link layer is the one which is responsible for data frame detection, multiplexing of data streams, detection of error and medium access. In this the data are transmitted in an open insecure medium so these are vulnerable to attacks. The different types of attacks present in link layer are: collision, exhaustion and unfairness

**3.2.1 Collision**

Collision mainly occurs when two nodes simultaneously transmit in the same frequency. When those packets collide then there would be a small change in packet, and then would be acknowledged as mismatch at the time of checksum then they are scrapped and re-transmitted. One of the methods to prevent this type of attack is the use of error correcting codes but these can be used only at a low level of collisions.

**3.2.2 Exhaustion**

In this the attacker confuses the channel by continuously requesting and transmitting. This results in starvation for other nodes as they cannot access the channels. This is usually done by sending a large number of RTS (Request to Send) packets to the channel. This may lead to multiple collisions and drainage of power. One of the possible solutions for this is to use Time Division Multiplexing. As in this nodes are given fixed time slots to transmit its contents.

**3.2.3 Unfairness**

Unfairness can be referred as repeated collision based or exhaustion based attacks. It can also be referred as a weaker form in the Dos. This kind of attack is a partial Dos attack but this result in degradation of performance. One of the methods to this type of attack is to use smaller frames, so that the nodes can use the channel for small duration only.

**3.3. Attacks in Network Layer**

The main aim of this attack is to find a path for efficient routing mechanism. In this the attacker creates a routing loop and then tries to attract or repel network traffic, create artificial routing messages, and annoy the network performance by modifying, spoofing or replaying routing information. There are various attacks in

WSNs this includes:

### 3.3.1 Sybil Attack

In many cases, the sensors in a wireless sensor network might need to work together to accomplish a task, hence they can use distribution of subtasks and redundancy of information. In such a situation, a node can pretend to be more than one node using the identities of other legitimate nodes. This type of attack where a node forges the identities of more than one node is the Sybil attack. Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve. Sybil attack can be performed for attacking the distributed storage, routing mechanism, data aggregation, voting, fair resource allocation and misbehavior detection. Basically, any peer-to-peer network (especially wireless ad hoc networks) is vulnerable to Sybil attack. However, as WSNs can have some sort of base stations or gateways, this attack could be prevented using efficient protocols. Douceur showed that, without a logically centralized authority, Sybil attacks are always possible except under extreme and unrealistic assumptions of resource parity and coordination among entities.

However, detection of Sybil nodes in a network is not so easy .In Figure1 demonstrates Sybil attack where an adversary node 'AD' is present with multiple identities. 'AD' appears as node 'F' for 'A', 'C' for 'B' and 'A' as to 'D' so when 'A' wants to communicate with 'F' it sends the message to 'AD'.

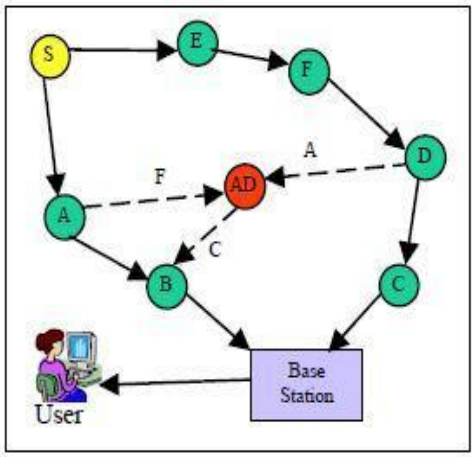


Figure 1. Sybil attack

### 3.3.2 Black Hole/Sinkhole Attack

In this attack, a malicious node acts as a blackhole to attract all the traffic in the sensor network. Especially in a flooding based protocol, the attacker listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. Once the malicious device has been able to insert itself between the communicating nodes, it is able to do anything with the packets passing between them. In fact, this attack can affect even the nodes those are considerably far from the base stations. Figure 2 demonstrates sinkhole attack where 'SH' is a sinkhole. This sinkhole attracts traffic from nearly all the nodes to rout through it.

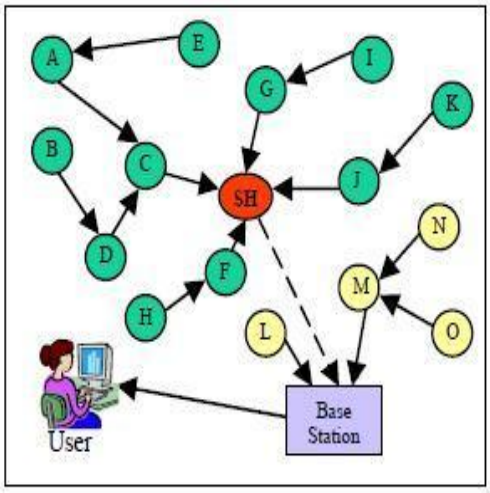


Figure 2. Blackhole Attack

The main reason for the sensor networks susceptible to sinkhole attacks is due to their specialized communication pattern. Sinkholes are difficult to defend in protocols that use advertised information such as remaining energy or an estimate of end-to-end reliability to construct a routing topology because this information is hard to verify.

**3.3.3 Hello Flood Attack**

Hello flood attack uses HELLO packets as a weapon to convince the sensors in WSN. In this sort of attack an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN. The sensors are thus persuaded that the adversary is their neighbor. As a consequence, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker. Figure 3 illustrates how an adversary node 'AD' broadcast hello packets to convince nodes in the network as neighbor of 'AD'. Though some node like I,H,F are far away from 'AD' they think 'AD' as their neighbor and try to forward packets through it which results in wastage of energy and data loss.

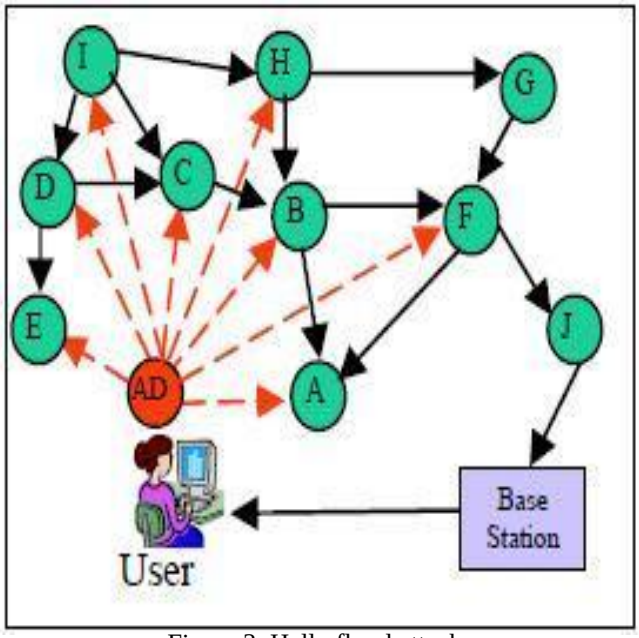


Figure 3. Hello flood attack

In a HELLO flood attack, every node thinks that the attacker is within one-hop radio communication range. If the attacker subsequently advertises low-cost routes, nodes will attempt to forward their messages to the attacker. Protocols which depend on localized information exchange between neighboring nodes for topology maintenance or flow control are also subject to this attack. HELLO floods can also be thought of as one-way, broadcast wormholes.

**3.3.4 Wormhole Attack**

Wormhole attack is a critical attack in which the attacker records the packets (or bits) at one location in the network and tunnels those to another location. The tunneling or retransmitting of bits could be done selectively. Wormhole attack is a significant threat to wireless sensor networks, because; this sort of attack does not require compromising a sensor in the network rather, it could be performed even at the initial phase when the sensors start to discover the neighboring information. Figure 4 demonstrates Wormhole attack where 'WH' is the adversary node which creates a tunnel between nodes 'E' and 'I'. These two nodes are present at most distance from each other.

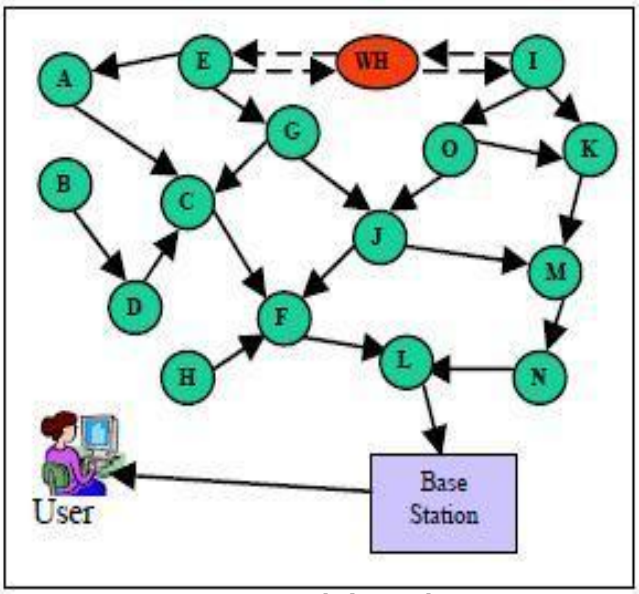


Figure 4. Wormhole attack

The simplest case of this attack is to have a malicious node forwarding data between two legitimate nodes. Wormholes often convince distant nodes that they are neighbors, leading to quick exhaustion of their energy resources. Wormholes are effective even if routing information is authenticated or encrypted. This attack can be launched by insiders and outsiders. This can create a sinkhole since the adversary on the other side of the wormhole can artificially provide a high quality route to the base station, potentially all traffic in the surrounding area will be drawn through her if alternate routes are significantly less attractive. When this attack is coupled with selective forwarding and the Sybil attack it is very difficult to detect. More generally, wormholes can be used to exploit routing race conditions. A routing race condition typically arises when a node takes some action based on the first instance of a message it receives and subsequently ignores later instances of that message. The goal of this attack is to undermine cryptography protection and to confuse the sensor's network protocols.

## IV. Security Solutions

There are many security issues arises in the wireless sensor networks. The issues related to the transmission of messages, on routing layer or physical node capture and size and density of the network. This becomes very challenging issue when we provide the security scheme to these networks. The different vulnerable data cause the security issues in the wireless sensor networks. Depending upon the attack this vulnerable data become the security threats. In this situation we are introduce the security services to the network; which ensures the protection of the information of information and resources from the attacks and threats.

The security challenges in the wsns lead to the different idea, which is the structure of the network, become more unfeasible and this will provide some security to the network. So here we are providing some security protocols for the competition of the security threats. As the other security mechanisms needs intensive computation and memory.

### 4.1 Spin (Sensor Protocols for Information via Negotiation)

The SPIN (Sensor Protocols for Information via Negotiation) was proposed by Adrian Perrig.the SPIN constitutes different building b blocks which optimized for resource constrain environments and w wireless communications. The building blocks in the SPIN is of two types; sensor network encryption protocol (SNEP) and μTESLA.the SNEP provides confidentiality, two party data authentication and data freshness. μTESLA provides authenticated broadcast for severely resource constraint environments.

The SPIN is a data centric routing protocol. The sensor node in the SPIN negotiates each and every node before sending the actual data using meta-data. The SPIN is basically a three way handshaking protocol which uses the three types of messages ADV, REQ and DATA. In the SPIN family includes various types of protocols, which includes SPIN-PP, SPIN-EC, SPIN-BC and SPIN-RL.

Table 1.SPIN and its characteristics

| *SPIN AND ITS TYPES* | *CHARECTERISTICS* |
|---|---|
| SPIN | User data negotiation and resource adaptive algorithm |
| SPIN-PP | Point to point transmission media |
| SPIN-EC | Add energy conservation heuristic to SPIN-PP |
| SPIN-BC | Single broadcast transmission media |
| SPIN-RL | Reliable version of SPIN-BC |

The above table explains the different versions and functions of the SPIN. From these we can understand that the SPIN protocol knows only about its single-hop neighbors .It saves more energy than other protocols. The ADV, REQ, AND DATA explain the different types of message in the SPIN. These will changes with environments and constraints of the communication.

**4.1.1 SPIN-PP:**

This protocol developed for establishing the point to point communication. The point to point communication is defined as the communication between two nodes with each other without interfering the other nodes. The below diagram explains the different phases in the SPIN-PP.

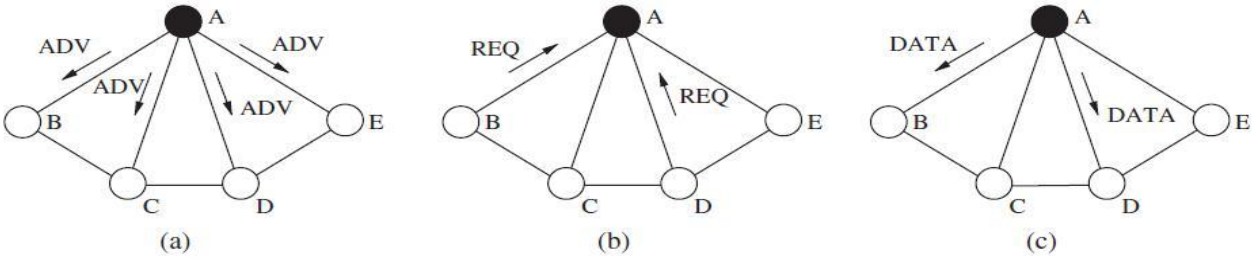


Figure 5. The SPIN-PP protocol: a) advertisement phase b) request phase c) data transmission

In the SPIN protocol; it broadcasts the ADV message to its neighbors when it receives the new data. The request message is generated when it needs the new generated data. DATA is the actual message generated when the actual data sent to the requesting nodes.

**4.1.2 SPIN-EC:**

It is the type of spin protocol in which the sensor nodes are communicating using the three way handshake protocol. The parameter which is added to this is energy conservation. That is when it receives the ADV message it will check the energy whether it is above or below the threshold energy.

**4.1.3 SPIN-BC:**

This protocol is designed for the broadcast channels where the network uses the same shared channels for the communication. In this protocol at a time we can send the information to the all other nodes. But there is a disadvantage for this that is it wastes the time and energy.

**4.1.4SPIN-RL:**

It is more reliable SPIN protocol. This protocol is developed by some modifications of SPIN-BC protocol. In this if the data does not received means it will again sends out the request. After sending the data the node will wait for some time before it responds to the other requests concerned about the same message.

**4.2 LEAP PROTOCOL**

The LEAP protocol is another security solution for wsns. The localized encryption and authentication protocol (LEAP) is the key management protocol used for providing security in the sensor networks. In LEAP

protocol four types of keys are assigned to each nodes; individual keys, pair wise keys, cluster keys and group keys. The advantage of this protocol is that it reduces the participation of base station and efficient in terms of communication and energy.

Table 2.Comparison between LEAP and improved LEAP

| ***FEATURES*** | ***LEAP*** | ***IMPROVED LEAP*** |
|---|---|---|
| Detects and removes compromised sensor nodes | yes | yes |
| Data loss | high | minimal |
| cost | low | high |
| Band width use | high | low |
| Transmission delay time | high | low |
| Energy consumption | high | low |
| Node life time | low | high |

The above table explains the different features of LEAP and improved LEAP. The improved LEAP overcomes the all problems of LEAP protocol.

**4.3 TINY-SEC:**

The TINY-SEC is defined as the link layer architecture for wireless sensor networks. It is the basis of higher level protocols and it is a fully executed link layer protocol of wireless sensor networks. TINY-SEC guarantees the message authenticity, confidentiality and integrity. It supports different types of CPUs and radio hardware.

In the networks there are many protocols are used for providing the security, such as IP/SEC, SSH and SSL. But these protocols are very heavy weight protocol for the sensor networks, as their packet formats and bytes of overhead does not support the sensor network environments. So the conclusion leads to the design of a new scheme with overcoming the problems of the existing scheme.

**4.3.1 DESIGN OF TINY-SEC:**

Tiny-sec design provides different security options; encryption, authentication and authentication with encryption. In the authentication mode it authenticates the data to the MAC, but in authenticated encryption it authenticates the entire packet and encrypts the payload with a MAC.

The authentication and encryption plays a key role in the design of tiny-sec.the MAC is computed over the encrypted data and the packet header. It also ensures that the information is received from a trusted node.

**4.3.2 ENCRYPTION:**

The encryption is defined as the converting plain text into the cipher text. Generally when the data is transmitting from the sender to the receiver the integrity of the message should be important. In these situations the encryption mechanism is introduced. That is the content should be read by the receiver after the decryption process of the text. Generally the plain text is converted into the cipher text. In encryption two design issues are there; encryption scheme and IV format.

**4.3.3 TINY-SEC IV FORMAT:**

The goal of our paper is to provide the security in a low cost. Here we can use two types of format, that is 1) too long or 2) too short. If we are using too long format means we can add the unnecessary packet and increase the throughput and energy drain. The too long packet contains the different data compared to the too short format. But when we are using the too short format we can add the any risks to the program and run it.

The structures of the IV format consist of destination address of the receiver, active message handle type, length of the data payload and source address. It also consists of ctr of 16 in number. That is this counter initiates when the data transmission initiates and it is incremented by the development of the data transmission.

**4.3.4 ENCRYPTION SCHEME:**

Here we are using cipher block chaining (CBC).it is the most appropriate mechanism for the wireless sensor networks. As when we are using the symmetric key encryption scheme, it cannot negotiate the too long packets and its payloads. In the network they are using the 8-bit for the transmission. The main goal of this scheme is to minimize the packet overhead.

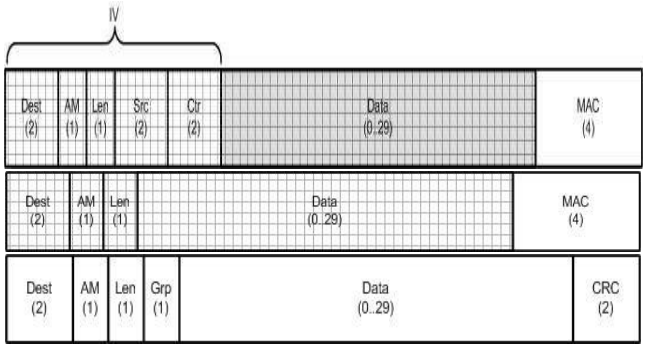


Figure 6. a) Tiny-Sec AE format b) Tiny-Sec Auth format c) Tiny-OS packet format

The above diagram explains the different packet formats of the tiny-sec design. In the packet contains the different features of the data. That is the destination address; it illustrates the data received by whom. The other feature includes the length and source address of the packet. The control bits are increased by each and every transmission

Table 3. Time to execute cipher operations on the sensor nodes

| ***CIPHER IMPLEMENTATION*** | ***TIME (MS)*** | ***TIME (BYTE TIMES)*** |
|---|---|---|
| Rc5 | 0.90 | 2.2 |
| Skipjack(C) | 0.38 | 0.90 |

Table 4: Total energy consumed to send 24 byte packets

| | ***ENERGY (MAH)*** | ***INCREASE*** |
|---|---|---|
| Current TinyOS stack | 0.000160 | --- |
| TinySec-AE | 0.000165 | 3% |
| TinySec-AE | 0.000176 | 10% |

The above table explains the execution time of cipher nodes and an energy consumed by the packet to send 24 byte packet. This will explain the different features of the nodes. In table 4. The energy is explained in terms of the different parameters. The TinyOS stack needed the 0.000160(mAH) amount of energy to send the packet. In the TinySec-AE shows the 3% of increase in the energy compared with the TinyOS.

The TinySec-AE provides 0.000176(mAH) of energy with 10% of increase compared to the others. The TinySec is cipher independent. In table 3.they given the Rc5 and skipjack; it can implemented at a time and switch between them without difficulty. The maximum data payload of TinyOS is 29 bytes and TinySec is currently released with the current tinyOS new versions. The TinySec increases the computational and energy costs of sending packet. Because it uses large size packet for transmissions extra computation time and energy is needed for the cryptography. The cryptography is defined as the process which encoding and decoding the message content during the transmission. The two types of cryptographic technique is; encryption and decryption. The encryption converts the plain text into cipher text (encoding) and decryption converts the cipher text into the plain text (decoding).

The table 5 illustrates the different keying mechanisms for link layer. Each keying mechanism shows its benefits and costs. The single network wide key is simple and easy to delay. But the group keys are shows graceful degradation in the presence of compromised nodes. It also prohibits passive participation and local broadcast.

Table 5.Summary of different keying mechanisms for link layer

| ***KEYING MECHANISM*** | ***BENEFITS*** | ***COSTS*** |
|---|---|---|
| Single network wide key | Simple, easy to deploy, support passive participation and local broadcast | Not robust to node compromise |
| Per link keys between neighboring nodes | Graceful degradation in the presence of compromised nodes | Needs a key distribution protocol, prohibits passive participation and local broadcast |
| Group keys | Graceful degradation in the presence of compromised nodes, prohibits passive participation and local broadcast | Requires key distribution; trades off robust needs to node compromise for added functionality |

## V. Conclusion

Security is becoming a major concern for energy constrained wireless sensor network because of the broad security-critical applications of WSNs. Sensor nodes which are deployed in hostile environments encounter a large variety of attacks and threats. Sensor networks are vulnerable to various attacks on different layers. In this paper, we have introduced various security issues, threats and attacks in WSNs and some defense mechanism. And in future, it is planned to evaluate more secure schemes and extend the framework.

## REFERENCES


[1] G. Abuaitah and B. Wang. "Secvizer: A security visualization tool for qualnet-generated traffic traces". In Proceedings of the 6th International Workshop on Visualization for Cyber Security (VizSec), VizSec '08, pages 111–118, 2009.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. "Wireless Sensor Networks: A Survey". Computer Networks, 38(4):393–422, Mar.2002.

[3] P. Bak, F. Mansmann, H. Janetzko, and D. Keim. "Spatiotemporal analysis of sensor logs using growth ring maps". Visualization and Computer Graphics, IEEE Transactions on, 15(6):913–920, nov.-dec.2009.

[4] S. Card, J. Mackinlay, and B. Shneiderman. "Readings in Information Visualization: Using Vision to Think". Morgan Kaufmann Publishers, San Francisco, 1999.

[5] Themistoklis Bourdenas and Morris Sloman. "Towards self-healing in wireless sensor networks". In Proceedings of the 2009 Sixth International Workshop on Wearable and Implantable Body Sensor Networks, pages 15–20, 2009.

[6] C. Charalambous and Shuguang Cui. "A biologically inspired networking model for wireless sensor networks". Network, IEEE, 24(3):6–13, 2010.

[7] Falko Dressler and Ozgur B. Akan. "Bio-inspired networking: from theory to practice".Comm. Mag., 48(11):176–183, 2010.

[8] Deborah Estrin, Ramesh Govindan, John Heidemann, and Satish Kumar. "Next century challenges: scalable coordination in sensor networks". In Proceedings of the 5th annual ACM/IEEE MobiCom, pages 263–270, 1999.

[9] S. Ganeriwal, A. Kansal, and M.B. Srivastava. "Self aware actuation for fault repair in sensor networks". In IEEE International Conference on Robotics and Automation, volume 5, pages 5244 – 5249, May 2004. Jessica Staddon, Dirk Balfanz, and Glenn Durfee. Efficient tracing

[10] R.Jurdak, X. R. Wang, O. Obst, and P. Valencia. "Wireless Sensor Network Anomalies: Diagnosis and Detection Strategies", chapter 12, pages 309–325. Intelligence-based Systems Engineering. Springer, 2011.

[11] E. Kandogan. "Visualizing multi-dimensional clusters, trends, and outliers using star coordinates". In Proceedings of the seventh ACM SIGKDD international conference on Knowledge discovery and data mining, KDD '01, pages 107–116, New York, NY, USA, 2001. ACM.

[12] D. A. Keim. "Information Visualization and Visual Data Mining". IEEE Transactions on Visualization and Computer Graphics, 8(1):1–8, Jan.2002.

[13] S. J. Simoff, M. H. B¨ohlen, and A. Mazeika, "Visual Analytics: Scope and Challenges", pages 76–90. Springer-Verlag, 2008.

[14] K. Lakkaraju, R. Bearavolu, A. Slagell, W. Yurcik, and S. North.C. "In NVisionIP: Integrating Discovery and Search in Security Visualization". IEEE Workshops on Visualization for Computer Security, pages 75–82, 2005.

[15] Al-Sakib Khan Pathan., Hyung-Woo Lee, Choong Seon Hong "Security in Wireless Sensor Networks: Issues and Challenges" proceedings from the 8th International Conference Advanced Communication Technology. ICACT 2006.pages 1043-1047.

[16] Murat Dener "Security Analysis in Wireless Sensor Networks", Hindawi Publishing Corporation International

Journal of Distributed Sensor Networks Volume 2014.

[17] Shio Kumar Singh, M P Singh, and D K Singh "A Survey on Network Security and Attack Defense Mechanism for Wireless Sensor Networks", International Journal of Computer Trends and Technology- May to June Issue 2011.

[18] Kalpana Sharma, Neha Mittal and Priyanka Rathi" "Performance Analysis of Flooding and SPIN in Wireless Sensor Networks.

[19] Delan Alsoufi, Khaled Elleithy, Tariq Abuzaghleh and Ahmad Nassar, "Security in wireless sensor networks - Improving the leap protocol", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.3, No.3, June 2012.

[20] Geetu, Sonia Juneja, "Performance Analysis of SPIN and LEACH Routing Protocol in WSN", International Journal of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5.