# Security Threats and its Countermeasures in Wireless Sensor Networks: An Overview

S.V.Annlin Jeba
Sr. Lecturer,
Department of CSE
CSI Institute of Technology,
Thovalai, Tamilnadu, India

B. Paramasivan
Professor and Head
Department of CSE
National Engineering College
Kovilpatti, Tamilnadu, India

D.Usha
Lecturer
Department of CSE
National Engineering College
Kovilpatti, Tamilnadu, India

## ABSTRACT

Wireless sensor networks (WSN) have lot of interest in research due to their wide range of typical application areas such as environmental, military and commercial enterprises. Sensor network possesses unique challenges to protocol builders, because these tiny wireless devices are often deployed in unattended environment with limited capabilities. Hence these networks are vulnerable to different types of malicious attacks. This paper surveyed the different types of attacks and security related issues in WSN. Moreover an analysis about some of the security protocols in two major domains namely, cryptography based protocols and en-route filtering schemes have been done.

**Keywords:** wireless sensor networks, security protocol, attacks, security services, en-route filtering.

## 1. INTRODUCTION

WSN [1] is formed by the collection of sensor nodes, each equipped with its own sensor, processor, radio transceiver and small memory with limited battery power. These nodes are capable of performing some processing, gathering, sensing and communication. Security is a common concern for any network system, but security in WSN is of great importance to ensure its application success. From the security standpoint, it is very important to provide data confidentiality, data authentication, data integrity, data availability, data freshness, time synchronization and secure localization [2]. Hence the QOS(quality of service) constraints such as memory, computational power, battery power, transmission range must be minimized so that the overhead caused by the security protocols can be light weighted [3]. All these security challenges are encouraging researchers to develop security protocols and algorithms suitable for WSN. Some of the security mechanisms are cryptography and key management, secure time synchronization, secure location discovery, secure routing, trust management system, **s**ecure data aggregation and intrusion detection.

This paper tells how to provide authentic and accurate data to surrounding sensor node and to the sink. Authentic and accurate data is provided to surrounding sensor node through cryptographic scheme and to the sink through en-route filtering scheme. Cryptography includes techniques to hide information in storage or transit. Some of the security protocols such as SPINS, Tinysec, LEAP, LEDS, LCG based light weight protocol, MiniSec, MASA and VEBEK use cryptographic proficiency to secure data. En-route filtering means that not only the destination node but also the intermediate nodes can check the authenticity of the message in order to reduce the number of hops the bogus message travels and, thereby conserve energy. Further the major features of these security protocols have been analyzed.

## 2. ATTACKS ON WSN

An attack is an event that diminishes or eliminates a network's capacity to perform its expected function and an adversary is a person or another entity that attempts to cause harm to the network by unauthorized access or denial of service. In WSN an attacker can falsify local sensor values in the area of WSN and may be able to mislead monitors in those areas. So a sensor node is not able to communicate and coordinate with the network and it is disrupted. Attacks [4] against wireless sensor networks could be broadly considered from different levels of views.

An outside attacker is a malicious node, not part of the network, but wants to harm the network, whereas an inside attacker is the one that is inside the network authorized to access the system resources but uses them in a way not approved by the granted authorization. Remote attack can be implemented from a large distance, for instance, by emitting a high-energy signal to interrupt the communication. A passive attacker just eavesdrops or monitors the packets that are transferred in a WSN. An adversary directly influences packets in the network through active attack as the fabrication of additional packages or suppression of existing packets.

In physical layer jamming is a common attack that can be done by adversaries by knowing the wireless transmission frequencies used in WSN. The attacker who uses its radio to listen the frequency and sends his own signal interfering with the message is called as collision attacker. Selective forwarding is an attack where compromised or malicious node just drops packets of its interest and selectively forwards packets to minimize the doubt to the neighbor nodes. In Sinkhole attack adversary attracts the traffic to a compromised node. A type of attacks where a node create multiple illegitimate identities in sensor network either by fabricating or stealing the identities of legitimate nodes is called Sybil attack. In a wormhole attack an adversary records information at an origin point and retransmits the information in the neighborhood of the destination.

Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network. Node compromise allows the adversary to enter inside the perimeter of security. While sending the report, the information in transit may be attacked to provide wrong information base stations or sinks. Here two major security schemes such as cryptography and en-route filtering are discussed.

# 3. CRYPTOGRAPHY BASED SECURITY PROTOCOLS

Cryptography is a standard method of defense against attack. It is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication. Most security protocols are based on cryptographic operations [5] that involve keys. Security of cryptographic system relies on secrecy of the key [6] it uses. Sender and receiver are required to update the key, time to time. To provide confidentiality an encryption operation is required. To guarantee authenticity the source node attaches a MAC to each packet. This section introduces selected security protocols such as SPINS, Tinysec, Minisec, LEAP, LEDS, LCG based light weight protocol, MiniSec, MASA, VEBEK of WSN.

## 3.1 Tinysec:

Tinysec [7] is a link layer security mechanism that can detect unauthorized packets when they are first injected into the network. This protocol guarantees authenticity, integrity, confidentiality. Tinysec support two different security options one is authenticated encryption other is authentication only. A common technique for achieving semantic security is to use a initialization vector (IV). Unauthenticated messages are vulnerable to attack but Tinysec always authenticate messages. Tinysec uses cipher block chaining construction, CBC-MAC for computing and verifying MAC.CBC-MAC is efficient, fast and minimizes the number of cryptographic primitives. The security of CBC-MAC is directly related to the length of the MAC. Tinysec's CBC-MAC is 4 byte long and then an adversary has 1 in $2^{32}$ chances in blindly forging a valid MAC for particular message. Tinysec uses a 8 byte IV, the first four bytes represent designation address and length. The last four bytes represent the source address and 16 bit counter starting with zero. CBC mode [8] of encryption is selected for Tinysec because of its robustness to information leakage when IVs repeat.

Tinysec is not tied to any specific keying mechanism. The keying mechanism can be selected based on the type of application the wireless sensor network will be used for. The drawback of Tinysec is Tinysec packets are longer than normal WSN packets. So extra computation and energy are needed for cryptography. The communication channel is slow, latency is increased since longer packet has to be transmitted. When compared with SPINS protocol data freshness cannot be achieved in Tinysec. Tinysec does not attempt to protect against replay attacks. Tinysec acts as a research platform for many other projects because of integrating Tinysec with existing applications requires only few changes to the application code thus enhance the security mechanism.

## 3.2 Spins:

SPINS [9] has two secure building blocks: SNEP and µTESLA .The goal of SPINS protocol is to design a key establishment technique based on SNEP and µTESLA to prevent the adversary from spreading to other nodes in the network through compromised node. SNEP provides the security primitives data confidentiality, two-party data authentication, data freshness. µTESLA provide broadcast authentication for resource constrained environment. These protocols are implemented on minimal hardware. SNEP provide low communication overhead, since it adds only 8 bytes per message. Like other cryptographic protocols such as Tinysec it uses a counter, but avoids transmitting the counter value. SNEP achieves semantic security which prevents eavesdropper from inferring the message content from the encrypted message. To achieve two-party authentication and data integrity a message authentication code (MAC) is used. SNEP offers properties such as Semantic security, data authentication, replay protection, weak freshness, low communication overhead.

The protocol µTESLA provides efficient authenticated broadcast. µTESLA overcomes the problem of high computation, communication and storage overhead by introducing asymmetry through the delayed disclosure of symmetric key. To send an authenticated packet and the base station computes a MAC on the packet with a key that is secret at that point in time. When a node gets a packet, it can verify that the corresponding MAC key was not yet disclosed by base station. Since the receiving node trust that the MAC key is known only to the base station, it assures that no adversary can have altered the packet in transit. This protocol does not address the problem of information leakage through secret channels. Broadcasting and authentication are not very easy for individual nodes, as storing a one-way key chain in node's memory is not possible. This scheme does not deal completely with compromisation. This protocol includes µTESLA overhead from releasing keys after certain delay, possible message delay.

## 3.3 Leap:

Localized Encryption and Authentication protocol. LEAP [10] is a key management protocol for sensor networks that is designed to support in–network processing. LEAP includes multiple keying mechanisms and restricts the security impact of a node compromise to the immediate network neighborhood of the compromised node. The design of this mechanism is motivated by the observation that different types of messages exchanged between sensor nodes have different security requirements and single keying mechanism is not suitable for meeting these different security requirements. LEAP supports four types of key for each sensor node. LEAP also includes a protocol for broadcast authentication. LEAP is designed to support security service such as confidentiality and authentication. The pairwise key establishment scheme includes computational overhead. The communication overhead for establishing a pairwise key includes an ACK message which has node id and MAC. The Hello messages exchanged between nodes to generate a pairwise key are not authentic. An adversary may exploit this to launch resource consumption attack by injecting large number of hello messages.

In LEAP broadcast authentication is achieved by using a one-way key chain. Whenever a node has data to send it attaches a key along with the message. Authentication keys are disclosed in the reverse order of their generation. The computational cost increase with increase in size of the network. The communication cost for cluster key updating will also be based on the density of the network. An adversary may launch a selective forwarding attack in which a compromised node drops the packets containing the routing information of selected nodes and forwards other packet normally. LEAP reduces the effect of this attack by using local broadcast scheme. LEAP can also minimize HELLO FLOOD attack by making the nodes receive packets only from authenticated neighbours. LEAP can also be used to prevent sinkhole attack by providing unique ID authentication for each node in WSN. In LEAP adversary cannot launch a wormhole attack after key establishment as at that point every node has knowledge about its neighbours so it is not easy to convince a node that it is near a particular compromised node.

## 3.4 Minisec

Minisec [11] is a network layer security mechanism which operates in two modes: MiniSec (U), unicast designed for single-source communication, and MiniSec (B), tailored for multi-source broadcast communication. MiniSec claims low energy utilization and memory usage. This protocol guarantees data confidentiality, authenticity, data freshness and replay protection. MiniSec uses similar packet format as TinyOS and replaces the 2-byte CRC from TinyOS with a 4-byte tag, as the tag protects the packet from tampering. MiniSec also eliminates the need of 1-byte group ID and uses different cryptographic keys. MiniSec is the first fully-implemented general purpose security protocol for the Telos sensor motes.

Both Tinysec and SNEP have developed solutions for providing secure communication in the unicast setting. Although both protocols attempt to minimize energy consumption, there are aspects of both that demonstrating inefficient energy usage. Tinysec uses an encrypted counter as its IV. This counter is appended to each message, resulting in a 2-byte overhead per packet. SNEP also uses a counter as the IV. However, SNEP conserves energy consumption by not sending the counter with each packet. MiniSec was able to decrease a security overhead of 5 bytes by Tinysec to 3 bytes Thus our secure sensor network communication package, MiniSec, offers a high level of security while requiring much less energy than previous approaches like Tinysec, SPINS.

## 3.5 LCG based lightweight security protocol

A lightweight block cipher [12] based on Linear Congruential generator (LCG) is a lightweight secure protocol for resource-constrained WSN. The term 'light weight' means procedure takes less computation power and consumes less energy. The light weight block cipher which is suitable for WSN can reduce computation overhead and increase the overall performance of security protocol. One type of light weight security protocol is light weight block cipher based on linear congruential generator.LCG based security protocol provide security services such as hop-by-hop confidentiality, integrity, authentication of data messages. The reason that we select the LCG is because it is the simplest, most efficient, and a well-studied pseudorandom number generator. The pseudo-random number generated by LCG to decide about the numbers needed for successful encryption use plumstead's algorithm. The message to be encrypted is delimited into segments of 1 byte.

Authentication and integrity are achieved through a MAC mechanism. A four byte MAC is used and an adversary has 1 in $2^{31}$ chances in forging a valid MAC for a particular message. In this protocol encryption process involve less operation. So an adversary can launch replay attack by eavesdropping on message sent between two nodes. An approach to overcome replay attack is to include a counter shared between two nodes with the transmitted message. No message overhead is involved in the process. Encryption operation alone cannot resist the plaintext attack. To solve this, permutation function applied to encrypted data change the original order of the encrypted message. Even though the operations involved are simple and less, the computing cost is more compared to the block cipher RC5 because of the costly operations involved in LCG algorithm such as 128 bit multiplication and 128 bit modulo. This protocols can be can be used in other environment and with other application to achieve maximum security.

## 3.6 Location aware end to end data security: LEDS

This protocol provides end-to-end data security .In LEDS [13], the targeted area is divided into multiple cells. After deployment the location information about the node can be known by a localization scheme [2]. The objective of LED is to guarantee confidentiality, authentication of data report. In addition it provides high level of assurance of data availability by protecting the data from report disruption attack and selective forwarding attack.

When an event occurs in a cell, it can be detected by sensor nodes within the cell and they generate a report about that event and forward this report to the sink node, which aggregates the data collected from different sensor nodes. The report can be secured as no node in the event cell gets compromised. The report is endorsed by number of sensing nodes and authenticated by nodes in different cells along the report forwarding route and also by the sink node. The encrypted report is divided into number of unique shares. Each share is independently generated by the participating nodes using its secret key shared with sink.MAC is then computed for all the shares, which enables en-route filtering. When the report is received by the sink node, it checks if the report contain't+1' valid non zero MAC. If true the report is accepted otherwise rejected. The report disruption attack can be avoided by dividing the encrypted report into number of unique share. In selective node capture attack, the attacker has to compromise atleast t nodes from one particular cell to compromise data authenticity of that cell and compromised nodes from one cell cannot be used to compromise authenticity of other cells. The main advantage of LED is its report endorsement mechanism and its forwarding mechanism.

## 3.7 Mixture of asymmetric and symmetric approach: MASA

MASA [14] is a security system with a combination of symmetric and asymmetric cryptography to provide end-to-end data security for WSNs. This method ensures that the content of the message is not altered maliciously or accidentally. The technique used for forwarding the event message is different from that of LEDS. In LEDS at each hop in the forwarding path old MAC has to replace by new MAC. But in MASA the event report is signed by the private key of the sender and only the sink has the corresponding public key to decrypt the encrypted event report. Computation performed at each hop in the forwarding path in LEDS is more complicated. No computational overhead occur in MASA. Strong data authenticity is achieved by the use of a list of trusted neighbours and helper nodes to control the data movement between source and sink. Thus MASA improves some of the weakness of LEDS.

## 3.8 Virtual energy-based encryption and keying for wireless sensor network: VEBEK

VEBEK[15] is a secure network protocol for wireless sensor Network (WSN ).This protocol minimizes the overhead associated with refreshing keys and uses a one-time dynamic key for one message generated by the source sensor. VEBEK uses RC4 encryption mechanism to provide simple confidentiality of the packet. The key to the encryption is obtained from Virtual Energy based keying module. The receiving node must keep track of the energy of the sending node to decode and authenticate a packet.

When a forwarding node receives the packet, it checks its watch list to determine if the packet came from a node it is watching. If not the packet is forwarded without modification. VEBEK supports two operational modes VEBEK-1 and VEBEK-11. In VEBEK-1 mode all nodes watch their neighbors. When a packet is received from a neighbor sensor node, its authenticity and integrity are verified. VEBEK-I reduce the transmission over head as it can catch malicious packets in the next hope itself. But increases processing overhead because of the decode/encode that occurs at each hop. In VEBEK-II operational mode, node in the network is configured to only watch some of the nodes.

## Security Analysis:

The salient features possessed by each protocol are: The protocol VEBEK is an energy efficient security protocol.LED is known for its secure localization. Protocol LEAP meant for attack minimized to neighborhood. Minisec is known for the use of offset code book for encryption.SPINs protocol is used in resource limited environment. TinySec possess link layer security architecture. Tinysec is not limited to any particular keying mechanism like LEAP but it is simple enough to integrate to any application. It is more efficient than TinyOS in terms of energy consumption. Figure 1 shows the memory consumption of protocols such as SPINS, Tinysec, Minisec, LEAP and VEBEK. Protocols SPINS occupy 2KB memory and protocol LEAP occupy 17.5KB memory.

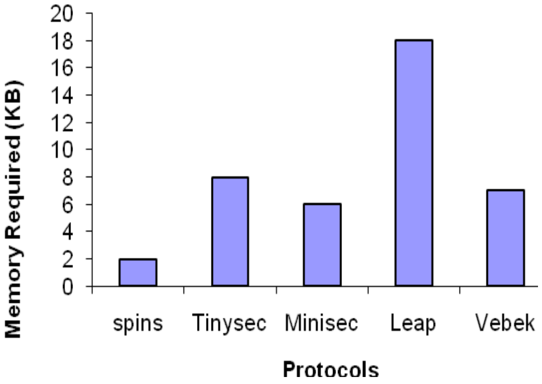

**Figure 1.Memory requirement of different security protocols**

SPINS guarantees security services such as confidentiality, authentication, data freshness and data integrity. Confidentiality is achieved by encryption through RC5 algorithm. µTESLA provides authenticated broadcast in SPINS. Key setup operation in SNEP is more expensive when compared to protocol VEBEK. LEAP [10] is designed to support in–network processing. LEAP require four types of key for each sensor node. It also includes a protocol for broadcast authentication as in SPINS and it is specially designed to support security service such as confidentiality and authentication. Figure 2 shows the bandwidth requirement of security protocols. Protocol SPINS transfer data at the rate of 30bytes per second. TINYSEC transfer data at the rate of 80 bytes per second. LEDS include location aware key management framework to the reduce the impact of compromised node. LEDS achieves the security services such as confidentiality, authentication, data availability by the unique secret key shared between node and the sink. LEDS increases the communication cost since every authentic report contains T+1 MACs. LCG based protocol guarantees the security services such as confidentiality, authenticity and integrity. Confidentiality is achieved by the pseudo random number generated by the linear concruential generator along with permutation function. LCG play an extra role in altering the original order of the content of the message. This protocol is known for its simplicity and efficiency. MASA is used to provide end-to-end security as LEDS between source and the sink. MASA provides the security services integrity, confidentiality, authentication and availability. MASA is used to improve some of the weakness of LEDS. Computation performed at each hop in the forwarding path in LEDS is more but no computational overhead occur complicated in MASA.VEBEK is an energy efficient secure network protocol for WSN when compared to Tinysec, LEAP, Minisec. VEBEK is able to efficiently detect and filter false data injected into network by malicious outsiders. VEBEK provide the security services such as confidentiality, authenticity and data integrity. VEBEK is able to detect false injection and eaves dropping of message from an outside malicious node. Figure 3 specifies the message overhead occurs in each message transfer of cryptography based security protocol. VEBEK occupies minimum overhead and LED occupies maximum overhead.

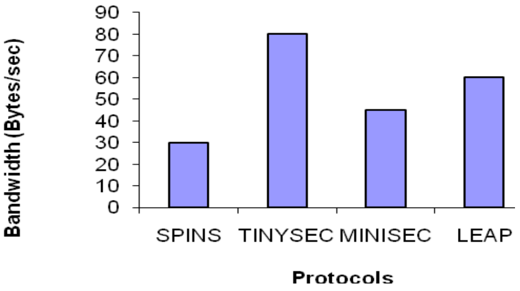

**Figure 2.Bandwidth occupied by different security protocols**

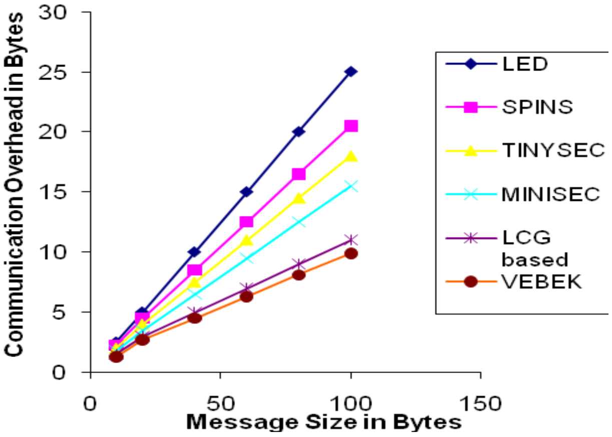

**Figure 3 Overhead incurred in each data transfer of security protocols**

## 4. EN-ROUTE FILTERING SCHEMES:

In WSN internal attacks are not detectable by cryptographic techniques. The unattended operation make it easy to compromise the sensor node and to release the information to the adversary .Adversary can launch internal attack that cannot be solved by cryptographic technique. Such internal attacks can be solved by en-route filtering scheme. En-route filtering means that not only the destination node but also the intermediate nodes can check the authenticity of the message in order to reduce the number of hops the bogus message travels and, thereby, conserve energy. Hence, it is especially useful in mitigating false data injection attack and path based DOS attack because the falsified messages will be filtered out as soon as possible.

## 4.1 Statistical en-route filtering (SEF):

Statistical en-route filtering (SEF)[16]is the first en-route filtering scheme proposed by F. Ye, H. Luo to address the fabricated report injection attacks in the presence of compromised nodes and introduce an en-route filtering framework. Each event detecting sensor endorses the report by producing a keyed MAC using one of its stored keys.. A report with insufficient number of MACs will not be forwarded. When the sink receives event reports, it can verify all the MACs carried in the report because it has complete knowledge of the global key pool. False reports with incorrect MACs that pass through en-route filtering will then be detected. The SEF mechanism (Statistical En-Route Filtering) detects and drops bogus reports from compromised nodes. The verifying of MACs is done probabilistically. SEF can't detect which nodes are compromised because reports are filtered en-route probabilistically, but it can prevent the false data injection attack with 80 - 90 percent probability within 10 hops. Otherwise this method is not very efficient.

## 4.2 An interleaved hop-by-hop authentication scheme (IHA):

Zhu et al. proposed an interleaved hop-by-hop authentication (IHA) scheme [17]. In this scheme, the base station periodically initiates an association process enabling each node to establish pairwise keys with other nodes that are n hops away, which is a security threshold. All nodes are detecting nodes and forwarding nodes, generating reports about events, forwarding them, and verifying report correctness. At least t+1 nodes must agree on a report for it to be considered valid. IHA requires the existence of a fixed path for transmitting control messages between the base station and every cluster-head. The high communication overhead incurred by the association process makes IHA unsuitable for the networks whose topologies change frequently.

## 4.3 Commutative cipher based en-route filtering (CCEF):

Yang et al. presented a commutative cipher based en-route filtering (CCEF) scheme [18]. In CCEF, each node is preloaded with a distinct authentication key. When a report is needed, the base station sends a session key to the cluster-head and a witness key to every forwarding node along the path from itself to the cluster-head. The report is appended with multiple MACs generated by sensing nodes and the cluster-head. When the report is delivered to the base station along the same path, each forwarding node can verify the cluster-head's MAC using the witness key. The MACs generated by sensing nodes can be verified by the base station only. CCEF has several drawbacks. First, it relies on fixed paths as IHA does. Second, it needs expensive public-key operations to implement commutative ciphers. Third, it can only filter the false reports generated by a malicious node without the session key instead of those generated by a compromised cluster-head or other sensing nodes.

## 4.4 Location-based resilient security (LBRS)

Yang et al. proposed a location-based resilient security (LBRS) scheme [19]. In LBRS, a sensing field is divided into square cells, and each cell is associated with some cell keys that are determined based on the cell's location. Each node stores two types of cell keys. One type contains the keys bounded to their sensing cells to authenticate the reports from those cells. The other type contains the keys of some randomly chosen remote cells, which are very likely to forward their reports through the node's residing cell. The authors introduced several types of report disruption attacks in which adversaries can intentionally attach invalid MACs to legitimate reports to make them dropped by other nodes. However, they did not provide a concrete solution. In addition, LBRS suffers a severe drawback: It assumes that all the nodes can determine their locations and generate location-based keys in a short secure time slot. However, to the best of our knowledge, most of the practical sensor localization approaches [2] cannot be finished in such a short time slot, and even the localization process itself is vulnerable to various attacks

## 4.5 Dynamic en-route filtering (DEF) scheme:

In the Dynamic En-route Filtering (DEF) scheme by Yu and Guan [20][21], a legitimate report is endorsed by multiple sensing nodes using their own authentication keys. Before deployment, each node is preloaded with a seed authentication key and secret keys randomly chosen from a global key pool. Before sending reports, the cluster head disseminates the authentication keys to forwarding nodes encrypted with secret keys that will be used for endorsing. The forwarding nodes stores the keys if they can decrypt them successfully. Each forwarding node validates the authenticity of the reports and drop the false ones. Later, cluster heads send authentication keys to validate the reports. The DEF[20] scheme involves the usage of authentication keys and secret keys to disseminate the authentication keys; hence, it uses many keys and is complicated for resource-limited sensors.

## 4.6Secure ticket-based en-route filtering:STEF

Secure Ticket-Based En-route Filtering (STEF) [22], proposed by Krauss et al., uses a ticket concept, where tickets are issued by the sink and packets are only forwarded if they contain a valid ticket. If a packet does not contain a valid ticket, it is immediately filtered out. STEF is similar in nature to SEF and DEF. The packets contain a MAC and cluster heads share keys with their immediate source sensor nodes in their vicinity and with the sink. The downside of STEF is its one way communication in the downstream for the ticket traversal to the cluster head

## Analysis about en-route filtering schemes:

Many en-route filtering schemes have been proposed to reduce false data injection attack in WSN. The statistical en- filtering (SEF) scheme, is the first to address false data injection attack. SEF has limited filtering capacity and cannot prevent impersonating attacks [24]. In SEF single shared key is used for generating and verifying MACs[23]. Hence keys may be misused to generate reports. To avoid this problem, a secure ticket-based en-route filtering (STEF) Scheme was introduced with ticket concept. Here a MAC on the report uses a key shared between the en-route node and the BS.STEF produce some additional overhead due to query-response communication for the ticket traversal. But the storage requirement is very less and STEF can be used in high density network. The IHA defines a new concept of association among sensor nodes. IHA guarantees that the BS will detect any injected false data packages when no more than t nodes are compromised. In IHA there is only one path from the Source cluster to the BS. Alternate paths are not available. In

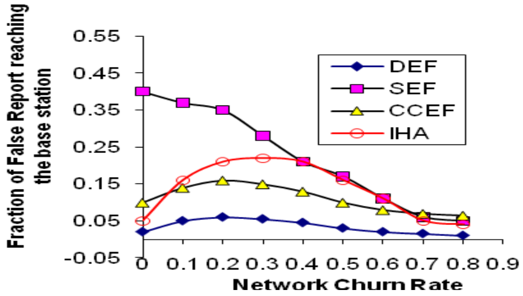

**Figure 4. Filtering capacities of different dynamic environments with different network chunk rate**

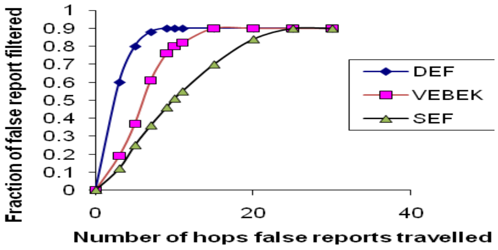

**Figure 5. Fraction of false report filtered as a fraction of number of hops they travelled**

CCEF the intermediate forwarding nodes are equipped with witness key which is used to verify the authenticity of the reports. But CCEF has several drawbacks. It relies on fixed paths as IHA does and it needs expensive public-key operations to implement Commutative ciphers. Figure 4. shows the average filtering capacity of different schemes in dynamic environment that have different churn rates. From the figure we know that DEF has higher filtering capacity. The curve corresponding to SEF

**Table 1. Case study on some of the security protocol**

| **Protocols** | **Number of prestored keys** | **Encryption scheme** | **Authentication mechanism** | **Resilience to Node capture** | **Attacks prevented** | **Security services provided** |
|---|---|---|---|---|---|---|
| **Tinysec** | one | RC5 Block Cipher+ Initialization vector | CBC-MAC | One in $2^{31}$ Chance can Forge correctly | Replay protection,<br>Link layer collision | Message integrity,<br>Confidentiality |
| **SPINS** | one | CTR-RC5 | μTESLA | Captured node send false message to BS | Replay Attacks are prevented | Confidentiality,<br>Authentication,<br>Data freshness |
| **Lightweight Protocol** | Three | Lightweight Block cipher (pseudo random number + permutation) | CBC-MAC | One in $2^{31}$ Chance can Forge correctly | Eavesdropping,<br>Avoid injecting Falsified message | Message integrity,<br>Confidentiality,<br>Authentication |
| **LEAP** | four | RC5Block Cipher | MAC, one way Hash function | Encryption using three key avoid revealing the message | Sybil, Hello flood,<br>Worm hole attack | Confidentiality,<br>Authentication |
| **LEDS** | Three | Event report Encrypted With cell key | Report Authentication key | Compromising will not break the confidentiality of report | Report disruptions,<br>Selective forwarding | Confidentiality,<br>Authenticity,<br>availability |
| **MASA** | Two | Private key, one way hash function. | Hash code,<br>Message Digest | No node get affected if less than T nodes are compromised | Selective forwarding | Message integrity,<br>Confidentiality,<br>Authentication |
| **VEBEK** | one | RC4 block cipher | Permutation code | The virtual energy used for key generation avoid revealing the message | Outside attacks (replay,<br>Brute force attack) | Authentication,<br>integrity,<br>non repudiation |

is flat which means these DEF and SEF are independent of topology changes. Moreover SEF can only filter the false reports generated by a malicious node without the session key instead of those generated by a compromised [25] cluster-head or other sensing nodes. Figure 5. shows the fraction false report filtered with the number of hops they traveled. DEF can filter 90% of false report within 5 hops. SEF can drop 90% of false report within 25 hops and VEBEK can filter 90% of false report within 15 hops. LBRS suffers a severe drawback: It assumes that all the nodes can determine their locations and generate location-based keys in a short secure time slot. In LEDS, the reports are forwarded through cells along report-auth routes. Each node stores the authentication keys shared between its cell and others in its downstream report-auth area and on the report-auth route. DEF is more complicated than SEF by introducing extra control message and the use of these control message not only increases operation complexity, but also incurs extra overhead. DEF is complicated for resource limited sensors

## 5. CONCLUSION

This paper presents the security relevant issues of WSN.A literature review about the security requirements, various possible attacks on WSN are described. Finally an analysis about the existing security protocols such as SPINS, Tinysec, LEAP, LEDS, LCG based light weight protocol, Minisec, MASA and VEBEK has been performed. The prons and cons of the existing protocols are discussed. Although several cryptography based security protocols have been proposed for security, those proposed solutions cannot prevent false reports injection by outside attackers. To address such problems in the presence of compromised sensor nodes en-route filtering schemes are essential. Also an analysis about these en-route filtering scheme is made in this paper. A case study is provided as a guidance to select the suitable security protocol.

## 6. REFERENCES

[1] I.F.Akyildiz Su, Y. Sankarasubramaniam, ”A survey on sensor Networks”,IEEE communication magazine vol.40,no.8,pp.102-114,Aug 2002

[2]. Daojing He,Lin cui,Hejiao Hang,”Design and verification of Enhanced secure localization scheme in wireless sensor network “IEEE Transaction On parallel and distributed systems vol. 20 no.7 July 2009

[3]. S. Uluagac, C. Lee, R. Beyah, and J. Copeland, “Designing Secure Protocols for Wireless Sensor Networks,” Wireless Algorithms, Systems, and Applications, vol. 5258, pp. 503-514, Springer, 2008

[4] Y. Wang, G. Attebury, B. Ramamurthy, A survey of security issues in wireless sensor networks, IEEE Communications Surveys & Tutorials 8 (2) (2006) 2–23.

[5] Yun Zhou,Y.fany,”securing wireless sensor networks a survey”IEEE communication survey & Tutorials vol. 10,no.3,2008

[6] Yang xiao, Venkata Krishna Rayi,Bo Sun,Xiao jiang Du,”A Survey of key management schemes in wireless sensor networks”Elsevier publication vol 30,pp2314-2341,2007

[7] C, Kerlof, N.Sastry, D.wagner”Tinysec, a link layer security architecture for wireless sensor networks”, proceeding of the second ACM conference on Embedded network sensor systems, 2004

[8] Yee Wei Law, Jeroen Doumen, Pieter Hartel, Survey and benchmark of block ciphers for wireless sensor networks, ACM Transactions on Sensor Networks (2006) 65–93.

[9] A perrig, R.Szewczyk, V.Wen, D.Culler and. J Tygar,”SPINS: Security protocols for sensor networks”ACM wireless networks vol 8, no 5, Sept 2002, pp 521-534

[10] Sencan Zhu, sanjeev setia, Sushil Jajodia,”LEAP: Efficient security mechanism for large scale distributed sensor networks”, Tech report (ACM), Aug 2004

[11] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, “Minisec: A Secure Sensor Network Communication Architecture,” Proc. Sixth Int’l Symp. Information Processing in Sensor Networks (IPSN ’07), pp. 479-488, Apr. 2007

[12] Bo Sun, Chung-chih Li, Kui,Wu, Yang Xiao,”A Light weight secure protocol for WSN”Elsevier computer communications vol 29,pp 2556-2568,2006.

[13]. K.Ren, W.Lou, Y.zhang,”LEDS: providing location aware End to End data security in wireless sensor networks”,IEEE Transactions on mobile computing Vol. 7, no. 5, may 2008.

[14] Alzcuid.H, Alfaraj.M, ”MASA: End to End data security in sensor networks using a mix of Asymmetric and symmetric approaches “IEEE conference mobility and security, vol 25,pp 1-5,2008

[15] Arif Selcuk Uluagac, Yingshu Li, ”VEBEK: Virtual Energy Based Encryption and keying for wireless sensor networks”IEEE Transaction on mobile computing vol. 9, No.7, July 2010

[16] F. Ye, H. Luo, S. Lu, and L. Zhang, “Statistical en-route detection and filtering of injected false data in sensor networks,” in Proc. IEEE INFOCOM, 2004, vol. 4, pp. 2446–2457

[17] S. Zhu, S. Setia, S. Jajodia, and P. Ning, “An interleaved hop-by-Hop authentication scheme for filtering of injected false data in sensor networks,” in Proc. IEEE Symp. Security Privacy, 2004, pp. 259–271.

[18] H. Yang and S. Lu, “Commutative cipher based en-route filtering in wireless sensor networks,” in Proc. IEEE VTC, 2004, vol. 2, pp.1223–1227.

[19] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, “Toward resilient security in wireless sensor networks,” in Proc. ACM MobiHoc, 2005,pp. 34–45

[20] Zhen Yu and Yong Guan ,”A Dynamic En-route Filtering Scheme for Data Reporting in Wireless Sensor Networks “ IEEE/ACM Transactions On Networking, Vol. 18, No. 1, February 2010.

[21] H. Hou, C. Corbett, Y. Li, and R. Beyah, “Dynamic Energy-Base Encoding and Filtering in Sensor Networks,” Proc. IEEE Military Comm. Conf. (MILCOM ’07), Oct. 2007

[22] C. Kraub, M. Schneider, K. Bayarou, and C. Eckert, “STEF: A Secure Ticket-Based En-Route Filtering Scheme for Wireless Sensor Networks,” Proc. Second Int’l Conf. Availability, Reliability and Security (ARES ’07), pp. 310-317, Apr. 2007.

[23] S. A. C¸ amtepe and B. Yener.,"Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks" In IEEE/ACM Transaction on Networking, vol. 15, no. 2, pp. 346-358,Apr,2007.

[24] Shahriar Mohammadi1 and Hossein Jadidoleslamy," a comparison of link layer attacks on wireless sensor networks", International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC)", Vol.3, No.1, March 2011.

[25] Garth V. Crosby, Lance Hester," Location-aware, Trust-based Detection and Isolation of Compromised Nodes in Wireless Sensor Networks", International Journal of Network Security, Vol.12, No.2, PP.107-117, Mar. 2011.

## 7. AUTHORS PROFILE

**S.V.Annlin Jeba:** did her master's degree in Computer Science and Engineering under Anna University Chennai, India. She is recently working as a Senior Lecturer in C.S.I. Institute of Technology, south India. Moreover she is a research scholar in Anna University Tirunelveli, south India.

**Dr.B. Paramasivan** received M.E degree in Computer Science and Engineering under Jadavpur University, Kolkatta, India. He obtained his Ph.D degree in Anna University, the area of research is Quality of Service in Wireless Sensor Networks. He is working as a Professor and Head in Department of Computer Science and Engineering, National Engineering College, Kovilpatti, Tamilnadu, India. He has published more than ten papers in International and National Journals. He has also presented more than fifteen papers in various International Conferences. He has organized more than ten seminars sponsored by various Governmental agencies. He is an active member of various professional bodies like IE and CSI.

**D.Usha** did her master's program in computer science department at MS University, Tirunelveli, south India . She is recently working as Lecturer at National Engineering College, Kovilpatti, south India. Moreover she is a research scholar in M.S. university Tirunelveli, south India