CHAPTER 2

LITERATURE SURVEY

Security attacks in Wireless Sensor Networks ranges from Denial of Service Attacks, Sybil attack, Black hole/Sinkhole attacks, Hello flood attack, Wormhole attack etc. Though several encryption schemes have been proposed to overcome data loss due to these attacks, the limited resources of the sensor nodes makes it impossible to opt for complex encryption mechanisms and hence multipath, randomized routing schemes were explored. The concept of multipath routing dates back to 1970s, when it was initially proposed to spread the traffic for the purpose of load balancing and throughput enhancement [Lee & Choi, 2006]. Later, the path-disjoint multipath routing gained popularity because of its usage in solving security issues. It also proved itself as a robust algorithm. Some of the protocols include, Split Multiple Routing (SMR) protocol [Boukerche et al. 2004], multipath DSR [Khushvinder&Shuang, 2009], and the AOMDV [Zhanet al. 2009] and AODMV [Greenwald& Khanna, 2004] algorithms that modify the AODV for multipath functionality. These protocols have been proposed very early and hence do not include the problem of security.

Attacks against wireless sensor networks could be broadly considered from two different levels of views. One is the attack against the security mechanisms and another is against the basic mechanisms (like routing mechanisms). The major attacks in wireless sensor networks are:
2.1 TYPES OF SECURITY ATTACKS

2.1.1 Denial of Service

Denial of Service (DoS) [Douceur, 2002], [Perrig et al. 2002] is produced by the unintentional failure of nodes or malicious action. In wireless sensor networks, several types of DoS attacks [Wang & Schulzrinne, 2004] in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and desynchronization. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic.

2.1.2 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 (Figure 2.1). This type of attack where a node forges the identities of more than one node is the Sybil attack [Ganesan et al. 2003], [Karlof & Wagner, 2003]. 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 [Karlof & Wagner, 2003].
2.1 Sybil Attack

2.1.3 Blackhole/Sinkhole Attack

In this attack, a malicious node acts as a blackhole [Shnayder et al. 2004] 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 2.2 shows the conceptual view of a blackhole/sinkhole attack.
2.1.4 Hello Flood Attack

Hello Flood Attack [Wang et al. 2008] uses HELLO packets as a weapon to convince the sensors in WSN. In this sort of attack an attacker with a high radio transmission (termed as a laptop-class attacker in [Wang et al. 2008] 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.

2.1.5 Wormhole Attack

Wormhole attack [Karlof & Wagner, 2003] 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 2.3 shows a situation where a wormhole attack takes place.

![Figure 2.3 Wormhole Attack](image)

2.2 ENCRYPTION SCHEMES

Data encryption is widely used to ensure security in open networks such as the internet. With the fast development of cryptography research and computer technology, the capabilities of cryptosystems such as of RSA and Diffie-Hellman are inadequate due the requirement of large number of bits. The cryptosystem based on ECC is the recent trend of public key cryptography. [Watro et al. 2004] presents the implementation of ECC by first transforming the message into an affine point on the EC, over the finite field GF(p).

Traditional schemes like RSA or ElGamal require considerable amounts of resources. This serves as a downside due to the fact that resources are limited when it comes to sensor networks. Hence, their usage in sensor networks is limited. Rabin's Scheme was introduced in 1979 in [Karlof & Wagner, 2003]. It is based on the factorization problem of large numbers and is therefore similar to the security of RSA with the same sized modulus. Rabin's Scheme has asymmetric computational cost. The encryption operation is extremely
fast, however decryption times are comparable to RSA of the same modulus. This asymmetry makes Rabin's Scheme especially interesting for our application. NtruEncrypt [Nachikethet al. 2003], was introduced in 1996 by Hoffstein, Pipher and Silverman. NtruEncrypt is a public key cryptosystem where security is based on the hardness of the Shortest Vector Problem (SVP) in a very high dimension lattice. It still uses relatively large operands, but it reduces the overall asymptotic complexity of the encryption operation to $O(n^2)$ compared to RSA's $O(n^3)$.

Newsome, J and others in 2004 introduce a Message Expansion Problem which can be solved by a Data Link-layer security architecture called ‘Cipher-text Stealing method’ for wireless sensor networks. Conventional security protocols tend to be conservative in their security guarantees, typically adding 16-32 bytes of overhead. With small memories, weak processors, limited energy, and 30 byte packets, sensor networks cannot afford this luxury. TinySec addresses these extreme resource constraints with careful design.

TinySec [Chris et al.2004], the link-layer security protocol proposes a CBC scheme called Skipjack along with a specially formatted 8-bytes initialization vector (IV) to encrypt the data[Xu & Liu, 1995]. Under the power and security aware protocol for sensor networks, [Tao et al. 2010] proposes the TEASR protocol which is based on TinySec and EAR. The proposed protocol is the extension of EAR in which the RREQ message includes the residual energy-level and hop counts of each node along with the path. Each intermediate node calculates the ARE from the source to itself. Then, intermediate node forwards a one RREQ message, which has the smallest ARE value, out of multiple received RREQ. The path that has the smallest EAR is finally selected.

According to these methods, considering both residual energy and hop counts, the proposed scheme selects the final path between the source and destination. Once the path is completely calculated, the destination sends back the RREP message to the source to notify a success in route establishment.

Lee and others [Lee et al. 2007] describe a framework to solve the security threats by designing an address based cryptography scheme. An ACS is a combination of Ad hoc node address and public key cryptography. ACS is a certificateless public key cryptography [Al-Riyami & Paterson, 2003] solution in that public keys of mobile nodes are directly
derivable from their known Ad hoc node address plus some common information. Thus, it eliminates the need for certificate-based authenticated public-key distribution essential in conventional public-key management schemes. ACS is an efficient construction method of address-based public/private keys cryptography, which not only ensures high-level authentication to node exchange information, but also enables efficient network-wide secure key update via a single broadcast message. It also provides general information about how to choose the secret key sharing parameters used with public key cryptography to meet desirable levels of security and authentication. The advantages of ACS over existing certificate-based solutions are justified through extensive simulations. The proposed scheme ACS gives a new innovation towards more effective and efficient security design for MANETs.

The concept of ID-based cryptography was introduced by Shamir in [Frank, 2002] to solve the main drawback of public key cryptography by removing the necessity of the certificates. In an ID-based system, the identity of users are used as their public keys and therefore there is no need to have this public key (i.e. the users’ identity) certified. The secret key is derived from the user’s identity together with the trusted authority, called the PKG’s secret key.

Nonetheless, this makes the system impractical since the PKG will know all the secret keys that the users have and therefore, the PKG can always impersonate any user. This inherent problem in ID-based cryptography is known as the key escrow problem, which makes the ID-based system only practical in a closed organization. An unconditional trust to the PKG is required and it is assumed that the PKG will not be malicious.

In fact, the improvements on the implementations of ECC primitives have allowed the existence of more complex PKC primitives in sensor nodes, such as identity-based cryptography (IBC). In IBC systems, only the identity of the sensors must be exchanged, and as a result there is no need to send either public keys or certificates. This saves energy as there is less data to be sent through the communication channel, although IBC is also very costly in terms of memory and CPU usage. One of the most optimal implementation of pairings executes the $\eta_T(P,Q)$ pairing on 1.71 seconds, requiring 4.17 KB of RAM and 23.66 KB of code size running on a 8 Mhz Texas Instruments’ MSP430 microcontroller [Challal et al. 2011].
While it would seem that this primitive is not useful in sensor nodes, there may be certain contexts where it could be useful, such as underwater sensor networks. As for hash functions, some standards like SHA-1 can be easily included in sensor nodes. An unoptimized implementation needs of 122 $\mu$s for digesting one byte [Kevin et al. 2006]. Elliptic curves are an algebraic structure, and their use for cryptography was first mentioned in [Van et al. 2010] and [Obadiah et al. 2011]. ECC feature properties which allow the setup of a problem similar to the well known discrete logarithm problem of finite fields – also known as Galois fields (GF). In recent years, ECC has attracted much attention as the security solutions for wireless networks due to the small key size and low computational overhead. ECC includes key agreement, encryption, and digital signature algorithms. The key distribution algorithm is used to share a secret key, the encryption algorithm enables confidential communication, and the digital signature algorithm is used to authenticate the signer and validate the integrity of the message.

The use of elliptic curves in public key cryptography was independently proposed by Koblitz and Miller in 1985 [Deng et al. 2002] and since then, an enormous amount of work has been done on elliptic curve cryptography. The attractiveness of using elliptic curves arises from the fact that similar level of security can be achieved with considerably shorter keys than in methods based on the difficulties of solving discrete logarithms over integers or integer factorizations.

Elliptic curve cryptography [Gang et al. 2007] makes use of elliptic curves in which the variables and coefficients are all restricted to elements of a finite field. For the interest of the readers, it is said that Elliptic curves are not ellipses. ECC normally starts with an affine point called $P_m(x, y)$. These points may be the Base point (G) itself or some other point closer to the Base point. Base point implies it has the smallest (x,y) co-ordinates, which satisfy the EC. A character in a message is first transformed into an affine point of the elliptic curve by using it as a multiplier of $P_m$.

Now to recover the information from the encrypted version, first we apply the decryption process of ECC, by applying the private key of recipient ($n_B$) on the first element ($k_G$). This is subtracted from the second element to recover $P_{ml}$. Lastly by using the discrete logarithm concept, it is possible to evaluate the ASCII value and thereby recover the plaintext.
Hence the keys are transformed over the EC field for both encryption and decryption. This promises to afford maximum security from intruders and hackers.

Blackertet al. in 2003 has presented an implementation of ECC over the field GF(p) on an 80 MHz, 32 bit RAM microprocessor along with the results. Kristin Lauter has provided an overview of ECC for wireless security [Ye et al. 2005]. It focuses on the performance advantages in the wireless environment by using ECC instead of the traditional RSA cryptosystem. Ray C., [Michael & Rahul, 2009] in his work has explained the design of a generator, which automatically produces a customized ECC hardware that meets user-defined requirements. Alessandro Cilardo et al explains the engineering of ECC as a complex interdisciplinary research field encompassing such fields as mathematics, computer science and electrical engineering [Tao et al. 2010]. C. J. McIvor et.al [Parnoet al. 2005] introduces a novel hardware architecture for ECC over GF(p).

The work presented by Gang Chen presents a high performance EC cryptographic process for general curves over GF(p) [Jewson et al. 2007]. The standard specifications for public key cryptography is defined in (IEEE p1363, 2000). The paper presented by [Kevin et al. 2006] outlines a brute-force attack on ECC implemented on UC Berkley's TinyOS operating system for wireless sensor networks [Estrin et al. 2003]. The attack exploits the short period of the pseudorandom number generators used by cryptosystem to generate private keys. An efficient and novel approach of a scalar point multiplication which originates from radix-4 Booths algorithm was proposed by SangookMoon[Swain&Sahoo, 2009]. The paper proposed by Jaewon Lee [Heet al. 2004], presents 3 algorithms to perform scalar multiplication on EC, defined over higher characteristic finite fields such as OEA. Liu Yongliang [Zhu et al. 2003] showed that Aydos et al.'s protocol is vulnerable to man-in-the-middle attack from any attacker but not restricted on the inside attacker. They propose a novel ECC based wireless authentication protocol. A comprehensive coverage of EC field with the in-depth mathematical treatment is given in [Maxemchuk, 1975]. Owing to these existing works on ECC and its popularity, it is proposed to implement the crypto system based on ECC for text based application. The proposed work can be extended to XML based application since the future middleware technologies are in the control of XML based documents which is purely based on text.
Wang and others in 2008 adopt three most widely used cryptosystems RSA, DSA and ECC, in this ECC offers the highest security among current public key cryptosystems. The finite fields GF(2<sup>m</sup>) based implementation of ECC is proposed by Anoop[Maxemchuk,1975], improving the efficiency by eliminating the multiplicative inverse operation in point addition and point doubling. The irreducible polynomial in binary field implementation is chosen to be trinomial or pentanomial if the implementation of ECC on binary field GF(2<sup>m</sup>) is efficient than the prime field GF(p) implementation.

**Table 2.1 Summary of Encryption Algorithms**

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Type</th>
<th>Key size</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES</td>
<td>Block Cipher</td>
<td>56 bits</td>
<td>Most Common, Not strong enough</td>
</tr>
<tr>
<td>TripleDES</td>
<td>Block Cipher</td>
<td>168 bits (112 effective)</td>
<td>Modification of DES, Adequate Security</td>
</tr>
<tr>
<td>Blowfish</td>
<td>Block Cipher</td>
<td>Variable(up to 448 bits)</td>
<td>Excellent Security</td>
</tr>
</tbody>
</table>

These chosen polynomials cause the polynomial reduction in binary field to run much faster than the modular reduction in prime field. The level of security offered by an ECC scheme is largely determined by the difficulty of solving the ECDLP over the group of EC.
points used within the scheme [Mavropodi et al. 2007]. This should be a prime order cyclic subgroup of points on a suitably secure elliptic curve.

EccM 2.0 proposed by David and others [David et al. 2008], employs much less memory than EccM 1.0. EccM 2.0’s running time beats that of Diffie-Hellman based on DLP, using keys with the order of magnitude smaller in size and much secure. [Marina & Das, 2001] have proved that the energy consumed by AES with 128-bit keys for data encryption and decryption is 1.62 $\mu J$/byte and 2.49 $\mu J$/byte respectively. Potlapally and et al. [Ganesan et al. 2002], have proven that the energy consumed by MD5 is 0.59 $\mu J$/byte.

Tung and et al. in 2006 [Ye et al. 2003] implemented AES on a sensor node based on the 8-bit Atmel ATmega 128L microcontroller running at 8 MHz. The implementation is based on Gladman’s code that was cited in the AES proposal. Their implementation can encrypt a 128-bit block of plaintext in 0.857ms.

Agah and others [Agah et al, 2005] present a Dynamically Secured Authenticated and Aggregation scheme by combining the public and symmetric key cryptography leads to increase in security, computational speed as well as reduces memory usage. It also incorporates data aggregation which reduces the in network processing and increases the nodes lifetime.

The proposed DSAA approach mainly includes the following steps: (i) Shared key generation using ECDH (ii) Key initialization (iii) Message encryption at source node (iv) Aggregation at intermediate nodes and (v) Decryption process at sink node.

SNEP [Sun et al., 2007] provides a number of unique advantages. First, it has low communication overhead since it only adds 8 bytes per message. Second, like many cryptographic protocols it uses a counter, but we avoid transmitting the counter value by keeping state at both end points. Third, SNEP achieves even semantic security, a strong security property which prevents eavesdroppers from inferring the message content from the encrypted message.

Finally, the same simple and efficient protocol also gives us data authentication, replay protection, and weak message freshness. SNEP offers the following properties:
**Semantic security:** Since the counter value is incremented after each message, the same message is encrypted differently each time. The counter value is long enough that it never repeats within the lifetime of the node.

**Data authentication:** If the MAC verifies correctly, a receiver can be assured that the message originated from the claimed sender.

**Replay protection:** The counter value in the MAC prevents replaying old messages. Note that if the counter were not present in the MAC, an adversary could easily replay messages.

**Weak freshness:** If the message verified correctly, a receiver knows that the message must have been sent after the previous message it received correctly that had a lower counter value. This enforces a message ordering and yields weak freshness.

**Low communication overhead:** The counter state is kept at each end point and does not need to be sent in each message.

μTESLA: Authenticated Broadcast requires an asymmetric mechanism otherwise any compromised receiver could forge messages from the sender. Unfortunately, asymmetric cryptographic mechanisms have high computation, communication, and storage overhead, which make their usage on resource constrained devices impractical. μTESLA [Sun et al. 2007] overcomes this problem by introducing asymmetry through a delayed disclosure of symmetric keys, which results in an efficient broadcast authentication scheme. The proposed TESLA protocol provides efficient authenticated broadcast, [Papadimitratos& Haas, 2006]. However, TESLA is not designed for such limited computing environments as we encounter in sensor networks.

SPINS [Perrig et al. 2002] design UTESLA to solve the following inadequacies of TESLA in sensor networks. TESLA authenticates the initial packet with a digital signature, which is too expensive for our sensor nodes. μTESLA uses only symmetric mechanisms. Disclosing a key in each packet requires too much energy for sending and receiving. μTESLA discloses the key once per epoch. It is expensive to store a one-way key chain in a sensor node. μ TESLA restricts the number of authenticated senders.

Node-to-Node Key Agreement Scheme establishes a shared secret session key SKAB with node B. Since A and B do not share any secrets, they need to use a trusted third
party S, which is the base station, KAS and KBS, respectively [Sun et al. 2007]. The following protocol achieves secure key agreement as well as strong key freshness:

\[
\begin{align*}
A &\rightarrow B : N_A, A \\
B &\rightarrow A : N_A, N_B, A, B, MAC(K_{BS}, N_A | NB | A | B) \\
S &\rightarrow A : \{SK_{AB}\}K_{AS}, MAC(K'_A, N_A | B | \{SK_{AB}\}K_{AS}) \\
S &\rightarrow B : \{SK_{AB}\}K_{AB}, MAC(K'_B, N_B | A | \{SK_{AB}\}K_{BS})
\end{align*}
\]

(2.1)

The protocol uses our SNEP protocol with strong freshness. NA and NB ensure strong key freshness to both A and B. The SNEP protocol is responsible to ensure confidentiality through encryption with the keys KAS and KBS of the established session key SKAB, as well as message authentication through the MAC using keys K'AS and K'BBS to make sure that the key was really generated by the base station.

SEF can probabilistically filter out false reports en-route. SEF exploits collective decision making by multiple detecting nodes, and collective false detection by multiple forwarding nodes in the dense deployment of large sensor networks.

SEF consists of three major components: (1) key assignment and report generation, (2) en-route filtering, and (3) base-station verification. The process of key assignment and report generation is as follows:

1. The base station (sink) maintains a global key pool of \(N\) keys \(\{K_i, 0 \leq i \leq N-1\}\), divided into \(n\) non-overlapping partitions. Each partition has \(m\) keys.

2. Before each sensor node is deployed, it stores randomly chosen \(k\) (\(k < m\)) keys from a randomly selected partition in the key pool.

3. When an event appears, multiple surrounding nodes can detect the event and a cluster head (center-of-stimulus node) is elected to generate the event report. Note that SEF assume that the same event can be detected by multiple nodes.

4. Each of the detecting nodes generates a keyed MAC \(M_i\) using the event report (for example, the location, the time, and the type of event) and randomly selected \(K_i\), one of its \(k\) stored keys.
5. The cluster head collects all the MACs from detecting nodes and attaches randomly chosen $T$ MACs to the report. This set of multiple MACs acts as the proof that the report is legitimate.

In en-route filtering, when the cluster head forwards the event report with multiple MACs toward the base station, intermediate forwarding nodes verify the correctness of the MACs probabilistically, and drop those with forged MACs en-route.

Due to the statistical nature of the detection mechanism, a few bogus reports with invalid MACs may escape en-route filtering and reach the base station. In base-station verification, the base station further verifies the correctness of each MAC and eliminates false reports that elude en-route filtering.

A secure scheme for creating the hopping sequence based on SEF for mobile WSNs has been proposed. The basic idea is to use multiple MACs generated by detecting nodes as a seed of the hopping sequence. In addition, although the original SEF is applied for static WSNs, mobile WSNs require dynamic routing to search and find pathways to the base station. Therefore, in the proposed scheme, SEF is carried out in the routing phase.

Cam et al. [Sun et al. 2007] propose an energy-efficient security protocol for wireless sensor networks by using symmetric key cryptography and their NOVSF code-hopping technique. They consider a hierarchical architecture of the network where data are routed from sensor nodes to the base station through cluster heads. The basic idea of their protocol is to implement two algorithms in the sensor nodes and in the base station which the sensor nodes and the base station would follow at the time of data transmission and reception. To address the issue of energy-efficient data aggregation with secure data transmission, ESPDA protocol [Szczechowiak et al. 2009] is proposed. In contrast to the conventional data aggregation protocols, ESPDA avoids the transmission of redundant data from the sensor nodes to the cluster head.

To make the data transmission and aggregation more secure, cluster head is not required to decrypt or encrypt the data received from the sensor nodes. On the whole, though [Sun et al. 2007] is an energy-efficient secure protocol, it increases the processing burden of the base station, and to support the associated ESPDA scheme, it requires more energy which literally ruins the gains of the original scheme.
Ye et al. [Koblitz et al. 1987] propose a SEF scheme to detect and drop false reports during the forwarding process. In their scheme, a report is forwarded only if it contains the MACs generated by multiple nodes by using keys from different partitions in a global key pool. According to their findings, SEF can drop up to 70% of bogus reports injected by a compromised node within five hops and reduce energy consumption by 65% or more in many cases.

2.3 CERTIFICATELESS CRYPTOGRAPHY

Ravi and others [Ravi et al. 2012a] present an idea of adopting certificateless public key encryption (CL-PKE) schemes over mobile ad hoc network (MANET). To implement CL-PKE over MANET and to make it practical, it incorporates the idea of Shamir’s secret sharing scheme [Shamir, A 1979]. The master secret keys are shared among some or all the MANET nodes. This makes the system self-organized once the network has been initiated. In order to provide more flexibility, it considers both a full distribution system and a partial distribution system.

In 2003, Al-Riyami and Paterson [Eduardo et al. 2007] proposed a new system known as certificateless cryptography. The idea of certificateless cryptography is to gather the strength of both the public key cryptography and ID-based cryptography and to avoid the drawbacks that these two systems have. In this system, there is a trusted authority called the Key Generation Centre that will need to generate a partial secret key for the users, given the users’ identity.

2.4 KEY MANAGEMENT SCHEMES IN WSN

2.4.1 Partially distributed authority scheme

Partially distributed authority scheme was firstly proposed by Zhou and Hass. In their scheme it is assumed that there is an OTTP constructing and distributing keys for all the nodes. The OTTP then generates certificates for all of the nodes and distributes them respectively. In Zhou and Hass’ scheme, those certificates are fully stored in each DCA node as well. This provides authentication from potential threads of unauthorized nodes. Any
unauthorized node does not have valid certificate, thus will not get key shares from DCA nodes.

2.4.2 Fully distributed authority scheme

A fully distributed authority scheme is a modification of partially distributed certificate authority scheme firstly proposed by Luo et al. [David et al. 2008]. This scheme also makes use of the \((n, t)\) threshold secret sharing scheme [Brakerskiet al. 2011].

The difference between Luo et al.’s model and Zhou and Hass’ model relies on the following: In Zhou and Hass’ model, DCA nodes are randomly selected from all the nodes while Luo et al.’s model uses all of the nodes in the MANET to form the DCA. The msk is shared among all the nodes and for this reason, this scheme is called ‘fully distributed’.

Firstly, an OTTP generates an RSA key pair mpk/msk. The mpk is shared in the MANET. The msk is divided into \(n\) shares; each part is a Secret Key (sk) for every node. Nodes’ Public Keys (pk) are created from those sks. Then the OTTP creates certificates signed with the msk for each node, in order to bind nodes’ unique ID with nodes’ public key. These certificates are unforgeable and are stored in every node in the network.

2.4.3 ID-Based distribution scheme

One of the Identity-based authority schemes was proposed by Boneh and Franklin [De et al. 2003], which is an upgraded solution to Zhou and Hass’ scheme. It replaced the DCA with a threshold PKG. Initially, users in the network will collectively form the PKG. This PKG will generate a pair of mpk/msk, and the msk is divided and shared among all the initial nodes. It is not stated in [Karlof& Wagner, 2003] how this PKG is formed nor how the msk is distributed. In [Lou et al. 2004], Van Der Merwe, Dawoud and McDonald designed an OTTP which is called centralized PKG to generate and distribute keys. After the initiation, the user’s identity is used as the user’s public key, while each PKG node will generate a part of this user’s private key, which is based on the user’s identity. In this way, each user needs to obtain \(t + 1\) parts of private key to retrieve the private key.

The scheme proposed in [Kim et al. 2008] provides a mechanism to compute the number of malicious packets from a large number of packets and they rely upon the probabilistic method to prevent Denial of Service attack. Through this scheme they were able
to achieve a much better overhead than the HCF computation method. The scheme in [Akkaya et al. 2004] uses a game theoretic approach to prevent Denial of Service attacks in wireless sensor networks. They use two approaches: UDSR, which incorporates the total utility of each route in data packets and the second approach, is based on a watch list where each node earns a rating from its neighbors. The scheme discussed in [Yuet et al. 2001] proposed a new mechanism which increases the difficulty of launching a low level Distributed Denial of Service attack against a wireless sensor network by using a remote access framework which includes a virtual home and a Distributed DoSDefense Server.

The proposed model in [Roman et al. 2008] uses the cluster adaptive rate limiting which makes use of host based intrusion detection techniques. These techniques reduced the energy consumption to an arbitrarily low level until the attack is lifted. The public key cryptography technique [Johnson et al. 2001] prevents a certain category of Denial of Service attacks that target to drain the battery energy in wireless sensor networks. They use an ECC based key generation scheme and combines it with the Denial of Service mitigation scheme. The scheme discussed in [Przydatek et al. 2003] proposes a multiuser Denial of Service containment and incorporates a signature based broadcast authentication scheme. The scheme in [Przydatek et al. 2003] is for distributed wireless sensor networks which prevents the possible Denial of Service attack whenever the packet has been intercepted using a broadcast key management scheme. There are a number of hashing computations and numerical calculations to falsify the first intercepted data packet. But the scheme manages to win time for broadcasting trusted message packets over the entire network.

All of WSN’s block ciphers are designed using a 16-round Feistel data block encoding scheme realized by two sub-blocks of data transformation using the round encoding function. Like many other symmetric block ciphers, DES is also a Feistel network (Schneier, 1996). In a Feistel network the plaintext is divided into two halves from the first round of computations which is repeated a number of times (i.e., in subsequent rounds).

The advantage of a Feistel scheme (Figure 2.4) is that the block cipher used is very difficult to breach by proportional of one round key enumeration (Moldovyan et al. 2007). So it is necessary to determine the requirements for one round cipher transformation during the Feistel scheme design. The pros and cons of this approach for a network are as follows:
Advantages of a Feistel approach to networks:

1. In a Feistel scheme we can encode and decode in one operation sequence. Encoding an algorithm modification is achieved by queuing a round of sub-keys using modification.
2. It minimizes software coding.

Disadvantages of a Feistel approach to networks:

1. In a Feistel scheme we have two parts, left and right, but only one part of the block is used for coding in one round. For example, if the block on the right side ($R$) is used for the first time in coding, the second one on the left side ($L$) is only used for exchanging places, and thus not all parts of the block are participating in the coding process.
2. Transformation is very simple because the round function $F$ depends only on two parameters ($L$ and round key $K_i$).

This Feistel scheme appeared long before modern crypto-attacks as the original cipher using a block structure. Its modified version is applied further to limited resource devices as well as embedded devices. From the original standard version it is seen that the unmodified version does not meet the new security requirement paradigm.

A proposal has been presented to use controlled permutation boxes for implementation of a Feistel scheme design for WSN security. DDP can be performed with the so-called CPB’s which are fast even if implemented in cheap hardware. CPB is one part of the
comprehensive forthcoming start of controlled operations in security applications (Moldovyan et al. 2005).

The main content of this concept is to create substitution and permutation elements of block ciphers. They provide highly accelerated program realization nonlinear transformations with a small volume of modifications. These transformations are realized by the whole large size data block at once (32 and more bits) and are managed by transcriptive data and the algorithm’s keys dynamically. CPB mechanisms and their implementation in block cipher methods provide high stability of such algorithms in modern crypto-attacks such as differential cryptanalysis (Moldovyan et al. 2007).

New approaches to enhance the security of wireless sensor networks have been proposed. Two randomized array transmission schemes (Figure 2.5) are developed to secure wireless sensor networks at the physical layer. Transmission secrecy can be guaranteed by either the inherent ambiguities of MIMO blind equalization or the intentionally created ambiguities. Perfect secrecy is shown to be realizable under certain conditions. The schemes do not require secret keys, and work under more relaxed assumptions than existing techniques. They are useful for secure wireless data transmission or key distribution in wireless sensor networks.

Figure 2.5 The block diagram of array transmission

It proposes a new physical-layer transmission technique to realize secrecy under more reasonable assumptions. We assume that the unauthorized user may have better received
signal quality and knows all the transmission protocols. There are no secret keys shared by the transmitters and the authorized user before transmission, and both of them have no knowledge of the unauthorized user.

It exploits two special properties of wireless transmissions for secure designs. First, signals received by the authorized sensor node (or user) and the unauthorized nodes (or user) are different because their channels are different. Second, channels between the transmitters and the authorized user can be reciprocal [Zhou et al. 1999].

Core protocols, refer to those network protocols that a sensor network needs in order to function properly. These protocols are: routing (transmitting a packet from one sensor node to another sensor node), data aggregation (briefing many sensor readings into one single piece of data), and time synchronization (synchronizing the clocks of the network). The behavior and the properties of these protocols are highly dependent on the characteristics of the sensor network application where they are running, because they must be adapted to the requirements of the scenario. As a result, there are many core protocols from where an application designer can choose the most optimal for his/her scenario.

2.5 SECURE ROUTING SCHEMES

Routing is one of the most important protocols of sensor networks. As sensor networks have an inherent distributed nature, the nodes must be able to forward the information to those devices that need it. Many, if not most sensor network protocols depend on the availability of a routing infrastructure. Its importance makes it a potential target for attackers: most of the attacks can be crafted to hinder the routing processes. As there are many types of routing strategies (e.g. flat routing, data-centric routing, hierarchical routing, location-based routing), it is necessary to find suitable security approaches for every strategy that take into account their specific properties. Nevertheless, it can be possible to define certain generic countermeasures that can provide some security properties to all strategies.

Zhu et al, in 2003 have proposed a Directed Diffusion routing protocol which is highly energy efficient since it is on demand and the node does not have to maintain global
information about network topology. Nodes can also do aggregation and caching, in addition to sensing.

Some of the existing countermeasures against routing protocol attacks are analyzed by both existing surveys [He et al. 2004] and by drafts of routing standards for sensor networks like Routing over Low power and Lossy Networks [Zhu et al. 2004]. Attackers trying to manipulate the routing discovery mechanisms (using HELLO flood and acknowledgement spoofing attacks) transmit their packets with a higher transmission power. Therefore, nodes can defend themselves by verifying that the link is truly bidirectional, using extra protection mechanisms such as onetime keys if needed. An adversary can also try to overload a sensor node with irrelevant messages, as the lifetime of sensor networks is highly tied to the number of exchanged messages. Nodes can lessen the effects of this attack by introducing traffic quotas if the network seems overloaded.

An evolution of a hardware technology makes it possible to deploy lightweight and multi-functional mobile devices in a real environment. WSN are representative networks using these tiny and low-power sensor devices. Two types of communications occur in sensor networks: one is between end nodes, and the other is between end node and base station (BS). Not only the resource-restriction, but also the security-critical applications and security functions play very important roles in WSN. Besides, because of physically low-power facilities in a sensor device, power efficient protocols are essential to maximize a lifetime of networks. [Tao et al. 2010] proposes a power and security aware protocol for sensor networks. It proposes the TEASR protocol, the routing protocol considers mutual authentication of between nodes and an energy information of each nodes.

The recently published protocols that consider the security issues include the SPREAD algorithm[David et al. 2008], [Papadimitratos et al. 2006]. This algorithm helps in finding the most-secure and node-disjoint paths. A modified Dijkstra algorithm can also be used to iteratively find the top-K most secure node-disjoint paths. The H-SPREAD algorithm [Lou& Kwon, 2006] is an enhancement of SPREAD. [Brakerskiet al. 2011] and [Frank,2002] presents distributed Bound-Control and Lex-Control algorithms that helps in computing the shortest multiple paths that helps to reduce performance degradation. [Van et al. 2010] and [Obaidat et al. 2011] provide better immunity towards attacks. Both works are based on a
similar cryptographic method: the secret keys used by sensor nodes are specific to their geographic locations, which limits the impact of a compromised node.

Other secure multipath routing algorithms include SRP [Banka T, et al., 2005], SecMR [Burmester&Le, 2004], Burmester’s approach [Seo et al. 2008], and AODV-MAP [David et al.2007]. The Secure Message Transmission mechanism proposed in [Wang et al. 2003] continuously updates the rating of the routes. The work in [Deng et al. 2007] studies two different ways of spreading an information packet into shares: secret sharing multipath aggregation and dispersed (message-splitting) multipath aggregation. To reduce unnecessary retransmissions and improve energy efficiency, the Gossiping algorithm [Kamvar et al. 2003] was proposed as a form of controlled flooding. Parametric Gossiping was proposed in [Brakerski et al. 2011] to overcome the percolation behaviour by relating a node’s retransmission probability to its hop count from either the destination or the source. A special form of Gossiping is the Wanderer algorithm [Brakerskiet al. 2011], whereby a node retransmits the packet to one randomly picked neighbour. The protocol proposed in [Challal et al. 2011] is a variant of the single path AODV routing protocol. The proposed algorithm establishes node-disjoint paths that have the lowest delays. This is achieved by interacting with various layers. This protocol also considers end to end delay as a parameter and hence we obtain a better result.

Further energy efficiency in WSN is emphasized in [Kevin et al. 2006]. It states that single path routing schemes are prone to delays and failures and hence loss of data. Hence the alternative is multipath routing. Multipath routing schemes distribute the traffic across multiple paths instead of routing all the traffic along a single path, which spreads consumed energy evenly across the nodes within the network, potentially resulting in longer lifetimes. REER [Kevin et al. 2006] uses the residual energy, node available buffer size, and Signal-to-Noise Ratio (SNR) to predict the best next hop through the paths construction phase. Two traffic allocation methods are followed in REER. The first method selects the best single path for transmission of data. Hence helps in reduction of cost. The second method splits the data and transmits it in different paths. Hence delay is avoided.

Zhan and others [Zhan et al. 2009] propose centralized node revocation in sensor networks. When the base station detects a misbehaving node, it broadcasts a message to
revoke that node. Chan, Perrig, and Song [Greenwald & Khanna, 2004] propose a localized mechanism for sensor network node revocation; in their approach, nodes can revoke their neighbors. F. Bouhafs [Douceur, 2002] and his colleges present a clustering scheme for wireless sensor networks based on semantic properties. It implements Semantization in Wireless Sensor Networks from another angle. They try to minimize the amount and range of communication as much as possible by developing a clustering scheme that involves only nodes that are relevant to a given query or task, and groups them in a cluster. Reference [Perrig et al. 2002] addresses the issues related to data integration in wireless sensor networks with respect to heterogeneity, dynamicity, and distribution at both the technology and application levels. The authors present and discuss a query processing algorithm which makes use of the semantic knowledge about sensor networks expressed in the form of integrity constraints to reduce network traffic overheads, improve scalability and extensibility of wireless networks and increase the stability and reliability of networks against hardware and software failures.

In EEUC to address the hot spot problem, author proposed an unequal clustering mechanism to balance the energy consumption among cluster heads [Shnayder et al. 2004]. Clusters closer to the base station have smaller sizes than those farther away from the base station, thus cluster heads closer to the base station can preserve some energy for the purpose of inter-cluster data forwarding. And an energy-aware multi-hop routing protocol is proposed for the inter-cluster communication in EEUC mechanism. [Xian & Qiaoliang, 2009] and [Wang et al. 2008] consider the problem of minimizing the effect of misbehaving or selfish nodes on routing through punishment, reporting, and holding grudges. These applications of these techniques to sensor networks, is promising; but these protocols are vulnerable to blackmailers.

Karlof & Wagner in 2003 present two building block security protocols optimized for use in sensor networks, SNEP and TESLASNEP provides confidentiality, authentication, and freshness between nodes and the sink, and u-TESLA provides authenticated broadcast.

To improve network security for WSNs, multipath routing strategies [Szczechowiak et al. 2009], [Lee et al. 2001], [Lee & Choi, 2006] have become a hot topic. It can generally be classified into two categories: 1) packet delivery, which directly transmits
packets by various paths [Lee & Choi, 2006]–[Douceur, 2002], and 2) share delivery, i.e., transforming each packet into shares and then forwarding shares along different routes [Perrig et al. 2002]–[Xian et al. 2009].

Packet delivery mainly focuses on discovering node-disjoint or edge-disjoint paths for transmission; thus, it can enhance the security and robustness of networks. In [Lee & Choi, 2006], the Split Multiple Routing protocol was proposed to establish two maximally disjoint routes by flooding the ROUTE REQUEST (RREQ) message to the entire network. In [Boukerche et al. 2004], the security of sensor network routing protocols was analyzed, and it was found that multipath routing strategies are one of the effective countermeasures for the selective forwarding attack. In [Khushvinder & Shuag, 2009], a MDT method was designed to counter the selective forwarding attack by dividing the sensor nodes into two data flow topologies. However, packet delivery duplicates the transmissions, which may lead to high energy consumption.

Normally, share delivery uses secret sharing to enhance the security of packet transmission. Based on a secret-sharing algorithm [Perrig et al. 2002], the adversary cannot decode the packet without intercepting a required number of shares. Therefore, the security performance of the network is improved. Moreover, as there is no need to duplicate packet transmissions, share delivery can significantly relieve the energy consumption of networks. In [Rivest et al. 1978], based on a distributed N-to-1 multipath discovery protocol and secret sharing, the hybrid multipath scheme (H-SPREAD) was designed to improve both the security and reliability of WSNs. In [Wang et al. 2008], a secure message transmission mechanism was proposed to continuously evaluate the performance of each route, and then, routing of subsequent shares is determined according to the rating of routes. These works focus on deterministic multipath routing strategies, i.e., the route computation is not changed under the same topology.

With random multipath routing protocols [Shnayder et al. 2004], [Xian & Qiaoliang, 2009], [Karlof & Wagner, 2003], share delivery can further strengthen and guarantee the security of packet transmission, even if adversaries acquire the routing strategy. In [Karlof & Wagner, 2003], a mathematical framework was presented for analyzing random-routing protocols. [Anfenget et al. 2012] jointly considers both network security and lifetime
issues while aiming at designing an efficient secret-sharing-based disjoint multipath routing scheme to enhance both the security and lifetime performance of WSNs.

One simple countermeasure to limit the effect of a compromised node trying to inject false data is to improve the resilience of the aggregation functions, as some functions (e.g. minimum, maximum, sum, average) are more insecure than others. The redundancy of some networks can be also used as a tool to detect fake or faulty readings that are too deviated from the average of the neighbourhood. While detecting problematic data is important, the main challenge of secure data aggregation [Alzaid et al. 2008] is to detect a misbehaving aggregator.

There are also solutions that discover whether the reports sent by a malicious aggregator are forged or not. In one approach [Lou et al.2004] the aggregator must create a proof of its neighbors’ data (e.g. using a Merkle hash tree), which will be used in a negotiation with the base station to demonstrate the authenticity of the data used to construct the report. Other approaches [Eduardo et al. 2007] take advantage of the density of sensor networks by using the nodes in the neighborhood of the aggregator as witnesses. Finally, it is also possible to filter the packets containing the report and the proofs in their way to the base station, hence decreasing the amount of traffic created by false aggregations (e.g. by using a Bloom filter [Karof& Wagner, 2003]).

Different hop–by–hop related works [Ray et al. 2005], [Sun et al. 2007], [Szczechowiaet al. 2009] assumes that data security is guaranteed by means of some key distribution schemes; for example SEDAN [De et al. 2003] proposes a secure hop–by–hop data aggregation protocol [Ozdemir& Xiao, 2009] in which each node can verify immediately the integrity of its two hops neighbors’ data and the aggregation of the immediate neighbors by means a management of new type of key, called two hops pairwise key. SEDAN [De et al. 2003] provides a totally distributed scheme to guarantee data integrity. The SEDAN performance, evaluated by means of ad-hoc simulation, shows a better behavior than other solutions, i.e., SAWAN [Ray et al. 2005], in terms of overhead and mean time to detection. All hop–by–hop proposed solutions are vulnerable because the intermediate aggregator nodes are easy to tamper and the sensor readings are decrypted on those aggregators. End-to-end
encrypted techniques overcome this weakness of hop-by-hop techniques. Notice that end-to-end secure data aggregation techniques also use a key scheme.

Some approaches [Zhou & Hass, 1999], [Koblitz, 1987] suggest to share a key among all sensing nodes and the Sink, the aggregator nodes have not the key because the aggregator nodes handle data without making any encryption/decryption operation. The limitation of such a solution is that the whole network is compromised in case the key is compromised in a sensing nodes. An alternative approach is represented by the adoption of public-key encryption [Zhan et al. 2009], but in this case the drawback is represented by a high computation consumption. After this short overview, notice that all proposed solutions are based on the adoption of encryption techniques, ad-hoc key distribution schemes [Greenwald& Khanna, 2004], [Douceur, 2002], [Perrig et al. 2002], authentication, access control solutions in a WSN. Our solution, instead, focuses on the system architecture adopting hybrid network architecture, composed of Wireless Sensor Network and Wireless Mesh network. More specifically, to guarantee data security a end-to-end secure data aggregation is used, but the aggregation operations are performed by mesh routers, reducing the power consumption of sensor nodes by means a sharing of functions.

Information fusion is commonly used in detection and classification tasks in different application domains, such as robotics and military applications. Lately, these mechanisms have been used in new applications such as intrusion detection and DoS detection within the WSN domain, simple aggregation techniques (e.g., maximum, minimum and average) have been used to reduce the overall data traffic to save energy.

Additionally, information fusion techniques have been applied to WSNs to improve location estimates of sensor nodes, detect routing failures and collect link statistics for routing protocols.

Routing paths in MANETs potentially contain multiple hops, and every node in MANET has the responsibility to act as a router [De et al., 2003]. Routing in MANET has been a challenging task ever since the wireless networks came into existence. The major reason for this is the constant change in network topology because of high degree of node mobility. A number of protocols have been developed to accomplish this task.
There are various mobility models such as Random Way Point, RPGM, Manhattan Mobility Model, Freeway Mobility Model, Gauss Markov Mobility Model etc that have been proposed for evaluation [Koblitz 1987; Douceur, 2002].

Several performance evaluation of MANET routing protocols using CBR traffic have been done by considering various parameters such as mobility, network load and pause time. Zhan and others [Zhan et al. 2009] have analyzed the AODV and DSR protocol using Group Mobility Model and CBR traffic sources. Zhan and others [Zhan et al. 2009] investigated that DSR performs better in high mobility and average delay is better in case of AODV for increased number of groups. Also Rathy and others investigated AODV and DSR routing protocols under Random Way Point Mobility Model with TCP and CBR traffic sources. They concluded that AODV outperforms DSR in high load and/or high mobility situations.

DSR is a reactive routing protocol i.e. determines the proper route only when packet needs to be forwarded [De et al. 2003; Lee&Gerla, 2001, Boukerche et al., 2004]. For restricting the bandwidth, the process to find a path is only executed when a path is required by a node (On-Demand Routing). In DSR the sender (source, initiator) determines the whole path from the source to the destination node (Source-Routing) and deposits the addresses of the intermediate nodes of the route in the packets. Compared to other reactive routing protocols like ABR or SSA, DSR is beacon-less which means that there are no hello-messages used between the nodes to notify their neighbors about their presence. DSR was developed for MANETs with a small diameter between 5 and 10 hops and the nodes should only move around at a moderate speed.

Backpressure routing [Scott Moeller, et al. 2010] is often better to route packets along paths that temporarily take them further from the destination, especially if these paths eventually lead to links that are more reliable and/or that are not as heavily utilized by other traffic streams.

The work in [Koblitz, 1987] [Lee&Gerla, 2001] [Sun et al. 2007] considers routing heuristics based on an estimated delivery cost, such as an estimate of the expected number of hops required to reach the destination along a traditional shortest path. Work in [Lee& Choi, 2006] develops analytical properties of related schemes, and energy-optimal
routing for transmission of a single packet is considered in [Boukerche et al. 2004] [Khushvinder&Shuang, 2009] via dynamic programming. However, when a stream of packets are to be transmitted, none of the above algorithms are throughput optimal or energy-optimal. Backpressure techniques of this type were first applied to multi-hop wireless networks by Tassiulas and Ephremides in [Zhan et al. 2009], where throughput optimal algorithms were developed using Lyapunov drift theory. Lyapunov theory has since been a powerful mathematical tool for the development of stable scheduling strategies for wireless networks and switching systems [Zhan, G et al., 2009]-[Xu& Liu, 1995], including our own work in [Wang et al. 2008]-[Xu& Liu, 1995] that applies backpressure concepts to solve joint stability and performance optimization problems, including energy efficiency and fairness. Related work on energy efficient wireless scheduling is developed in [Lou et al. 2004]-[David et al. 2008]. The work in [Zhan et al. 2009]-[David et al. 2008] does not consider the broadcast advantage of wireless networks, and assumes that all transmissions are fully reliable. Work in [Papadimitratos& Hass, 2007] considers backpressure in combination with network coding, and work in [Brakerski et al. 2011] considers backpressure strategies for cooperative transmission (where multiple nodes transmit redundant information simultaneously for a power enhancement at the receiver). Heuristic algorithms that combine multireceiver diversity with network coding are developed in [Frank, 2002], and complexity issues of cooperative transmission for line networks are discussed in [Van et al. 2010].

The two modes of wireless communication that can be used are: Infrastructure-dependent, and infrastructure-independent (ad-hoc) networks. The infrastructure independent networks, are more promising for contingency planning. The types of communication involved in an emergency system can be intra-organisational, multi-jurisdictional, and multidisciplinary [Lee& Choi, 2006]. For the mitigation of emergency operations there are three essential aspects described in [Boukerche et al. 2004] which are

1. **‘just-in-time’ logistics**, where the resources are available on the emergency scene instead of having each responder to look for the required equipment stockpiled somewhere,

2. **situational awareness**, where responders should be warned of possible menacing threats at earliest to minimize risks, and
3. **enhanced situational awareness**, which address issues such as coordination of operations by multiple agencies.

The call for emergency preparedness leaves ad hoc networks as an attractive tool for communication support mainly because of its ease of deployment, infrastructure-less and highly dynamic topology. This has incited projects like WIDENS [Khushvinder&Shuang, 2009] (Advanced Wireless Deployable Network System for Public Safety), a European project, and DAWN [Zhan et al. 2009] (Dublin Ad Hoc Wireless Network) project, aim at covering the whole city of Dublin, among others.

Mobile nodes, despite being energy constrained should provide continuous assistance to rescuers. However, since transmission implies high energy consumption, the ideal formula will be

1. for a mobile node to try transmitting only when the channel is available so as to escape collision and,
2. it should transmit at the lowest power needed such that the transmission range covers at most up to the receiver.

This has led to the development of power-aware routing protocols where some research focused on the implications of power consumption of nodes in an ad hoc emergency MANET [Greenwald& Khanna, 2004].

Zhan and others [Lee& Choi, 2006] propose a security architecture for WSN, based on lightweight public key cryptography, yet the available memory and processing power may not even be sufficient to hold the variables of an asymmetric cryptosystem. Perrig and others [Perrig et.al. 2002] propose a security component called SNEP that can be used for mote-sink message authentication in WSN. Link layer security architecture for WSN called TINYSEC is proposed in [Ray et al. 2005] to provide authentication and maintain confidentiality. Both these techniques [Ray et al., 2005; Sun et al. 2007] use symmetric key encryption which severely drains energy from the sensor nodes.

Sending the randomized data over wireless channel requires more energy. Therefore, [Perriget.al. 2002] [Sun et al. 2007] proposed a protocol to achieve semantic security using symmetric key encryption with the help of counter (CTR) shared between the
sink and the mote. Karlof and others [Karlof & Wagner, 2003] and Ray and others [Ray et al. 2005] have argued that if each counter requires 4-bytes and 100 bytes RAM available for the neighbor table, networks with larger than 25 nodes would be vulnerable. However, the careful observation makes clearer that neighbor table is to hold the counter shared with its neighbors only, but not with all the nodes in the network. Therefore, the CTR-based schemes do not face the scaling problem. Moreover, TINYSEC [Ray et al. 2005] consumes extra computation and communication overhead.

Levieil&Naccache in 2008 proposes a LIghtweight Security Algorithm (LISA) tailored to implement in resource restrained sensor nodes. The novelty of this scheme is that it achieves both, confidentiality and authenticity of data, without using traditional encryption algorithm. LISA is to achieve the same security services as proposed in SNEP [Sun et al. 2007] but in a reduced implementation complexity. LISA uses cellular automata (CA) -based operations because of the simple, regular and modular structure of the CA based component. The whole operation of LISA comprises of two basic phases: Initialization phase and Data authentication phase.

[Levieil&Naccache, 2008] achieves the following security properties.

- **Semantic Security:** Since the counter value is incremented after each data, the same data gives the different results even though with the same secret key. Therefore, the scheme achieves semantic security.
- **Mote (source) Authentication:** Verification is performed to check if the message has been generated from the correct mote. Thus sink authenticates the mote.
- **Replay Protection:** The counter value in the message prevents the replay of old messages.
- **Weak Freshness:** Sink correctly verifies that the message has been generated after the previous message. This assures the weak freshness.
- **Cut and Paste Attack Resistant:** If the attacker changes a part of message while flows from mote to sink, sink rejects the message as the implicit message integrity checking
is carried out at data authentication phase. Therefore, LISA is robust against Cut and Paste attack.

- **Message lost tolerant:** Since both the sink and mote use a common counter value and update without their confirmation, de-synchronization occurs if the message flows from mote to sink gets lost. In this situation, counter value at the mote that has incremented is not equal to that value stored at sink. In the next instance, of the protocol takes care of the lost message and therefore LISA is tolerant towards message lost.

- **Counter value de-synchronization protection:** If the message flows has been dropped more than once it is considered as intentional. Therefore, sink may take some appropriate actions and counter re-initialization phase is executed. Thus, the protocol is robust against de-synchronization attack.

Routing and energy efficiency are the main focus of the general routing protocols, however, the security issue is not considered [Rayet al. 2005], so the general routing protocols are vulnerable to various attacks. For example, GEAR [De et al. 2003] needs exchanging location information, so a malicious node can put itself on the routing path by broadcasting fake location information. If the malicious node participates in data transmission, it can perform many attacks such as the selective forwarding attack.

The multi-path routing mechanism proposed by Ganesan [Didla et al. 2008] can resist the selective forwarding attack. The main idea is to build multiple paths from the source to the destination, and transmit the copies of one packet on multiple paths. So long as there is no malicious node performing selective forwarding on one single path, the packet can be delivered to the destination.

INSENS proposed by Sun and others [Sun et al. 2007] limits the destruction of a malicious node to some extent. And it can continue providing routing service while not excluding the malicious node. SEF proposed by Szczechowiak and others [Szczechowiak et al. 2009] focuses on identifying false data. When an event happens, SEF elects one center node CoS from all the sensors which detect the event. CoS gathers all the detecting data and generate an integrated report. Then CoS broadcasts the report to all the sensors which detect the event. If the detecting node agrees with the report, then it generates a MAC and transmits
it to CoS. After CoS gathers enough MACs, it notifies the sink of the event. However, the event reports about which CoS haven’t gathered enough MACs will be abandoned.

Zhu and others in 2007 proposes an IHOP scheme in [Koblitz, 1987]. IHOP guarantees that the base station will detect any injected false data packets when no more than a certain number of nodes are compromised.

EASY [Lee&Gerla, 2001] adopts random detection mechanism to reduce the packets which need to be validated. Then the whole network load is decreased. But there is a strict limit to EASY. It’s that the routers and cluster heads can’t be captured.

[Ravi et al. 2012b] proposes SOAR, a secure route for the false data injection [Zhu et al. 2007] attack model. SOAR works in the stream data transfer mode and randomly detects the false data injection attacks. SOAR guarantees that the base stations receive small percentage of false packages with rather low load. The goal of SOAR is to try to avoid the false data injection attack, and at the same time increases little computation and low communication overload.

2.6 TRUST BASED ROUTING

Most existing routing protocols for WSNs either focus on energy efficiency [Abdelzaher et al. 2004] assuming that each node is honest with its identity, or they try to exclude unauthorized participation by encrypting data and authenticating packets. Examples of these encryption and authentication schemes for WSNs include TinySec [Szczechowiak et al. 2009], Spins [Greenwald et al. 2004], TinyPK [Perrig et al. 2002], and TinyECC [Lee & Choi, 2006; Liu&Ning,2008]. Admittedly, it is important to consider efficient energy usage for battery-powered sensor nodes and the robustness of routing under topological changes and common faults in a wild environment. However, it is also significant to incorporate security as one of the most important goals; meanwhile, even with perfect encryption and authentication, by replaying routing information, a malicious node can still participate in the network using another valid node’s identity.

In contrast, trust management [Zhou & Hass, 1999] has been introduced into peer-to-peer networks and general ad hoc networks to support decision-making [Sun et al., 2007, Douceur, 2002], improve security [Ray et al. 2005, Boukerche et al. 2004], and promote node
collaboration [Didla, et al. 2008] and resource sharing [Lee&Gerla, 2001]. Basically, trust management assigns each node a trust value according to its past performance. These studies target general ad hoc networks and peer-to-peer networks but not resource-constrained WSNs. Additionally, they do not address attacks arising from the replay of routing information.

With a similar idea, S. Ganeriwal, L. Balzano, and M. Srivastava also proposed a reputation-based approach to detect uncooperative nodes in WSNs [De et al. 2003]; however, they do not address the attacks by exploiting the replay of routing information.

TARF - a trust-aware routing framework for wireless sensor networks has been proposed. TARF identifies those malicious nodes that misuse “stolen” identities to misdirect packets by their low trustworthiness, thus helping nodes circumvent those attackers in their routing paths. Not only does TARF significantly reduce negative impacts from these attackers, it is also energy-efficient with acceptable overhead. It incorporates the trustworthiness of nodes into routing decisions and allows a node to circumvent an adversary misdirecting considerable traffic with a forged identity attained through replaying. It identifies such intruders that misdirect noticeable network traffic by their low trustworthiness and routes data through paths circumventing those intruders to achieve satisfactory throughput. TARF is also energy-efficient, highly scalable, and well adaptable.

To address the problem of security and efficiency in routing in WSNs, a scheme that reliably identifies compromised (or faulty) nodes and utilizes a routing path that avoids these nodes has been proposed. Essentially, it utilizes a single-path routing concept and thereby saves energy-consumption. If a malicious node is detected on the next-hop on the routing path, the node is efficiently bypassed and the packets are routed around the node to the base station still in a single-path. The protocol is an extension of the protocol presented in [Szczechowiak et al. 2009] and is more energy-efficient than the base protocol. It mainly concentrates on energy-efficiency and increased reliability, since the packets in the network are always routed in single-path avoiding costly multi-path approach.

2.7 INTRUSION TOLERANT PROTOCOLS

Most of the proposed schemes in WSN fail even if a single node is compromised, since they concentrate only on outsider attacks. An insider attack on a WSN is even more dangerous, since an attacker in this case can launch various types of attacks such as dropping
of legitimate packets, injecting of bogus packets and sensing reports, advertising false routing messages, eavesdropping on the network communication etc. Parao et al have proposed a distributed detection mechanism [Khushvinder&Shuang, 2009]. Newsome et al [Zhan et al. 2009] have presented some techniques for preventing an adversary from launching Sybil attack by arbitrarily creating new identities.

Deng et al. in 2002 have proposed an intrusion tolerant routing protocol in wireless sensor networks (INSENS) that adopts a routing-based approach to security in WSNs [Greenwald& Khanna, 2004]. It constructs routing tables in each node, bypassing malicious nodes in the network. The protocol cannot totally prevent attack on nodes, but it minimizes the damage caused to the network due to an attack. The scheme has reduced computation, communication, storage, and bandwidth requirements at the sensor nodes at the cost of greater computation and communication overhead at the base station. Tanachaiwiwat et al. have proposed a novel secure routing protocol- trust routing for location-aware sensor networks(TRANS) [Douceur,2002]. It makes use of a loose-time synchronization asymmetric key cryptographic scheme to ensure message confidentiality. Zhu et al have proposed a localized encryption and authentication protocol to prevent insider attacks--particularly message eavesdropping and message fabrication attacks [Perrig et al. 2002]. Compromised or faulty nodes may also drop legitimate packets by launching selective forwarding attacks [Zhou & Hass, 1999]. In order to defend against such type of attacks, most of the existing secure routing protocols in sensor networks are based on multi-path forwarding scheme [Rivest, et al.,197;Ganesan et al. 2003], or interleaved mesh forwarding scheme [Karlof & Wagner, 2003].

Zhu et al. [Lee &Gerla, 2001] propose the interleaved hop-by-hop authentication scheme that detects false reports through interleaved authentication. Their scheme guarantees that the base station can detect a false report when no more than ‘t’ nodes are compromised, where t is a security threshold. In addition, their scheme guarantees that ‘t’ colluding compromised sensors can deceive at most B non-compromised nodes to forward false data they inject, where B is O(t2) in the worst case. They also propose a variant of this scheme which guarantees B=0 and which works for a small t.
Motivated by [Lee & Gerla, 2001], Lee and Cho [Lee & Choi, 2006] propose an enhanced interleaved authentication scheme called the key inheritance-based filtering that prevents forwarding of false reports. In their scheme, the keys of each node used in the message authentication consist of the node’s own key and the keys inherited from its upstream nodes. Every authenticated report contains the combination of the message authentication codes generated by using the keys of the consecutive nodes in a path from the base station to a terminal node. Other than these works, [Boukerche et al. 2004; Khushvinder & Shuang, 2009; Zhan et al. 2009] focus only on energy efficiency in wireless sensor network, and the works like [Ray et al. 2005; De et al. 2003; Greenwald & Khanna, 2004] deal with the security measures for routing in WSN.

A protocol, which creates a tree structure in the network based on the energy levels and distances (from the base station) of the sensor nodes has been proposed. Along with the energy-efficient structuring of the network, it initializes an efficient security scheme down the paths of the tree to ensure secure data transmission in the network. This scheme addresses secure data transmission from the source sensors to the base station along with energy-efficient structuring and operation of the network. Deception through false injection of data is prevented. The forwarding nodes can detect the irregularities with a minimum effort and thus drop unnecessary or flawed packets. By stopping the false packets to travel a long distance along the created paths in the network, it helps for greater energy efficiency, as the intermediate nodes are thus saved from extra transmissions. Periodic restructuring of the network is proposed to keep a balance among the nodes to dissipate energies in nearly equal proportion.

A Public Key Infrastructure scheme for wireless sensor networks that tries to solve the problem of security in WSN by the use of public key cryptography as a tool for ensuring the authenticity of the base station has been proposed. RSA is composed of two phases, the first is the sensor to base station handshake in which the base station and a given sensor node setup a session key to secure end to end link between them, this handshake is protected and authenticated using the public key of the base station. The second phase is the use of this session key for data encryption to ensure confidentiality and ensuring the integrity of the exchanged data using the MAC joined to each packet.
A key distribution scheme, based on node layer security system, which combines with the group key distribution and identification of encryption has been proposed. This method can make the two nodes carry on communication in a secure environment when identified, at the same time, communication in the safe environment between groups can also be guaranteed. The results show that the ability of resistance to attack, Sybil attack, node increases the attack, the node replication attacks can effectively be stopped.

The Secure Energy-efficient Routing Protocol for densely deployed wireless sensor networks aims to achieve robust security for transmitted sensor readings with an energy-efficient network backbone. When the sensors with limited energy budgets are deployed in hazardous environment, ensuring energy efficiency and security of the sensor readings becomes a crucial task. It addresses how to deal with such a deployment scenario. This protocol ensures secure transmission of data from the source sensors to the base station in a way that it can best utilize the available amount of energy in the network. It uses one-way hash chain and pre-stored shared secret keys for ensuring data transmission security. In SERP, first, a sink rooted tree structure is created as the backbone of the network. This energy efficient network structure is used for authenticated and encrypted data delivery from the source sensors to the base station. To introduce data freshness, SERP includes an optional key refreshment mechanism which could be applied depending on the application at hand.

It also helps for energy-efficient structuring of the network so that the maximum lifetime of the network could be achieved.

2.8 PRIVACY HOMOMORPHISM TECHNIQUES

PH were introduced by Rivest, Adleman and Dertouzos in 1978 to solve the computing delegation problem in the first instance. This typically occurs when the data owner has only limited computing facilities, i.e. either the computation to be performed is too complex or an unmanageable bulk of data must be processed.

Other PHs are the Naccache-Stern public key encryption function [Lou et al., 2004], encryption transformations proposed by Benaloh [De et al. 2003], Lipton and Sander [Wang et al. 2008], and Domingo-Ferrer [Van et al. 2010]. The latter is an additive and multiplicative PH which is based on a symmetric cryptosystem. Although, in [Seo et al. 2008], Wagner showed that this PH is insecure for chosen plaintext attacks for some specific
parameter settings. Using this scheme for the WSN data aggregation scenario results in a higher level of security than solutions based on hop-by-hop encryption. For an adversary aiming to obtain confidential information, it is only reasonable to break a mechanism if the cost of breaking is less than the value of the revealed information. Nevertheless, more secure PHs are already available. Okamota and Uchiyama proposed a public-key cryptosystem with homomorphic properties, which is proven to be as secure as factoring [Eduardo et al. 2007]. However, the execution times for encryption and decryption are about twice as high as for elliptic curve cryptosystems, which is not acceptable for highly energy-restricted platforms.

2.9 DATA AGGREGATION TECHNIQUES

Castelluccia et al. presents an efficient aggregation of encrypted data in wireless sensor networks [Szczechowi et al. 2009]. This approach uses different keys per sensor node at the cost of mandatory transmitting of the sensor ID list of the encrypting nodes. Due to the increased message overhead per monitoring node, this approach does not scale for large sensor networks.

In [Rives et al. 1978], [Ganesan et al. 2003], some of the authors of this work introduce the concept of Concealed Data Aggregation (CDA), which is based on additive PHs in general and which we describe by using a specific PH from Domingo-Ferrer [Van ,et al. 2010]. CDA is the first work focusing on end-to-end encryption in WSNs by still providing in-network processing. The applied PH from Domingo-Ferrer is secure against adversaries that exclusively carry out chosen ciphertext attacks. However, in [Seo et al. 2008], Wagner shows that the scheme is vulnerable against chosen plaintext attacks based on an exhaustive search for certain parameter settings. In [Ganesan et al. 2003], when applying additive operations, e.g., to support aggregation functions like “average” or “movement detection,” the scheme is quite energy-efficient for a major class of WSN topologies. Nevertheless, a CDA scheme may, in principle, use any other symmetric and additive homomorphic PH. Rivest et al. [Frank, 2002] have proven that there is no PH which securely supports the minimum or the maximum operations in a secure way. [Zhou et al. 1999] adapts the Order Preserving Encryption Scheme (OPES) [Abdelzahe et al. 2004] by Agrawal et al. to CDA to also support comparison operations. The main drawback of the previously proposed CDA concept, for aggregation functions based either on additive operations or on comparison operation, is that the keying
model is based on a single network-wide shared key. Generally, such security approaches are not acceptable in WSNs where nodes can easily be corrupted and, consequently, the Dolev-Yao threat model [Khushvinder & Shuang, 2009] does not hold. For WSNs, this model needs to be extended to also address the capturing of sensitive data which is stored in the communicating end points. When combining encryption with the requirement of in-network processing, by still demanding a nonrestrictive election of aggregator nodes, most current solutions adopt hop-by-hop encryption and usually enforce a single network-wide key. Such is the case of security architectures of proprietary solutions like TinySec [Burmester & Le, 2004] or ZigBee [Challalet et al. 2011] atop the IEEE 802.15.4 [Wang & Vassileva 2003] standard, which are either based on RC5 or AES-CCM-64 (and other suites). Under such circumstances, the use of a single key for the whole network is probably the only possibility to guarantee a high routing flexibility. Here, the corruption of one node means that the attacker can subsequently eavesdrop on all the network traffic. [basepaper2] provides a symmetric PH for Concealed Data Aggregation, that applies an additive and symmetric reference privacy homomorphism.

The topology-aware key predistribution provides the best achievable security in an environment with non-tamper resistant devices and still ensures the application of CDA for reverse multicast traffic per RR.

The field of secure aggregation has still room for more improvements. Interactive protocols between aggregators and the base station require more traffic for the negotiation, introduce a delay in the aggregation service, and are not scalable without an aggregation testing hierarchy. Proof-based systems usually require a negotiation between the aggregator node and its witnesses and increase the size of the reports sent to the base station. New solutions should try to minimize the amount of negotiations carried out by these algorithms, and to introduce new ways to early detect and eliminate false reports.

In large WSNs, computing aggregates in-network (i.e., combining partial results at intermediate nodes during message routing) significantly reduces the amount of communication and hence the energy consumed. An approach used by several data acquisition systems for WSNs [Zhou et al. 1999], [Ray et al. 2005] is to construct a spanning tree rooted at the base station, and then perform in-network aggregation along the tree.
Tree-based aggregation approaches are not resilient to communication losses resulting from node and transmission failures, which are relatively common in WSNs. To address this problem, the research community has proposed the use of multipath routing techniques for forwarding subaggregates [Zhou et al. 1999]. For aggregates such as Min and Max, which are duplicate-insensitive, this approach provides a fault-tolerant solution. However, for duplicate-sensitive aggregates, such as Count and Sum, multipath routing leads to double-counting of sensor readings. Recently, several researchers [De et al., 2003], [Didla et al. 2008] have presented clever algorithms to solve the double-counting problem associated with multipath approaches. A robust and scalable aggregation framework called synopsis diffusion has been proposed for computing duplicate-sensitive aggregates, such as Count and Sum. This approach uses a ring topology where a node may have multiple parents in the aggregation hierarchy, and each sensed value or subaggregate is represented by a duplicate-insensitive bitmap called synopsis. However, most of the existing in-network data aggregation algorithms have no provisions for security. A compromised node might attempt to thwart the aggregation process by launching several attacks, such as eavesdropping, jamming, message dropping, message fabrication, and so on.

The TAG [Madden et al. 2002] to compute aggregates, such as Count and Sum, using tree-based aggregation algorithms were proposed in [Zhou et al. 1999]. Similar algorithms were proposed in [Ray et al. 2005]. Moreover, tree-based aggregation algorithms to compute an order-statistic have been proposed in [Szczechowiak et al. 2009]. Authors in [De et al. 2003] independently proposed very similar algorithms. These works use duplicate-insensitive algorithms for computing aggregates based on the algorithm in [Koblitz, 1987] for counting distinct elements in a multiset.

Several secure aggregation algorithms have been proposed assuming that the base station is the only aggregator node in the network [Lee&Gerla, 2001]-[Boukerche et al. 2004]. It is not straightforward to extend these works for verifying in-network aggregation unless we direct each node to send an authentication message to the base station, which is a very expensive solution. Only recently, the research community has been paying attention to the security issues of hierarchical aggregation.
A tree-based verification algorithm was designed in [Khushvinder & Shuang, 2009]–[Greenwald & Khanna, 2004] by which the base station can detect if the final aggregate, Count or Sum, is falsified. A verification algorithm for computing Count and Sum within the synopsis diffusion approach was designed in [Sun et al., 2007]. Recently, a few novel protocols have been proposed for “secure outsourced aggregation” [Douceur J., 2002]; however, these algorithms are not designed for WSNs. Although algorithms in [Sun et al., 2007], [Khushvinder & Shuang, 2009], [Zhan et al. 2009] and the verification protocol prevent the base station from accepting a false aggregate, they do not guarantee the successful computation of the aggregate in the presence of the attack. Some researchers also designed attack-resilient computation algorithms to empower the base station to filter out the false contributions of the compromised nodes from the aggregate. The first attack-resilient hierarchical data aggregation protocol was designed in [Perrig et al. 2002]. However, this scheme is secure when only one malicious node is present.

The attestation phase of SDAP [Greenwald & Kanna, 2004] can be expensively used to compute Count and Sum in the presence of a few compromised nodes [Yang et al. 2006]. Recently, an attack-resilient aggregation algorithm for computing Count and Sum has been proposed in [Rivest et al., 1978], which is based on a sampling technique. Despite the adversarial interference, this algorithm can produce a \((\varepsilon, \delta)\) approximation of the target aggregate.

Secure aggregation becomes especially challenging if end-to-end privacy between sensors and the Sink is required. In literature there are several works defined in order to guarantee security of the aggregated data. More specifically, the main contribution are cataloged into hop-by-hop [Ray et al. 2005], [Sun et al. 2007], [Szczechowia et al. 2009] and end-to-end [Zhou & Hass, 1999], [Koblitz, 1987] secure aggregation. In data aggregation the security issues, data confidentiality and integrity, become vital when sensor nodes are deployed in a hostile environment. In literature there are many works that address such security issues. These works have been classified in hop–by–hop encrypted data aggregation and end-to-end encrypted data aggregation. In the former the data is encrypted by the sensing nodes and decrypted by the aggregator nodes. The aggregator nodes, then, decrypt data coming from the sensing nodes, aggregate data and encrypt the aggregated data again. At last,
the Sink gets the final encrypted aggregation result and decrypts it. In the end-to-end encrypted data aggregation the intermediate aggregator nodes have not the key and can only do aggregations on the encrypted data.

Rivest et al. in 1978 presents a detailed review of in-network aggregation technique for wireless sensor networks. Aggregation techniques are an essential building block to keep the WSN operational as long as possible, as they aim to reduce the number of transmissions required for data collection, which, in turn, reduces energy consumption. Existing researches have been conducted to address pure data aggregation routing problem in WSN. In [Ganesan et al. 2003], they devise three interesting suboptimal aggregation heuristics, Shortest Paths Tree, Center at Nearest Source, and Greedy Incremental Tree for data centric routing problems. In [Karlof & Wagner, 2003], mathematical formulations for data aggregation problem in WSN are well formulated, and an optimization-based heuristic algorithm is then proposed to tackle the problem.

The ciphertexts in Gentry's fully homomorphic scheme [Lee & Gerla, 2001] contain a random 'noise' component that grows in size as the ciphertext is processed to homomorphically evaluate a function \( f \) on its plaintext [Gentry & Halvi, 2011; Gentry, 2009]. Once the noise size in the ciphertext exceeds a certain threshold, the ciphertext can no longer be decrypted correctly. This limits the number of homomorphic operations that can be performed. A method that provides two improvements to Gentry's fully homomorphic scheme based on ideal lattices and its analysis was proposed. It provides a more aggressive analysis of one of the hardness assumptions (the one related to the Sparse Subset Sum Problem) and a probabilistic decryption algorithm that can be implemented with an algebraic circuit of low multiplicative degree. Combined together, these improvements lead to a faster fully homomorphic scheme, with a \( O(\lambda^{3.5}) \) bit complexity per elementary binary add/mult gate. These improvements also apply to the fully homomorphic schemes of Smart and Vercauteren [PKC'2010] and van Dijk et al. [Eurocrypt'2010].

An encryption scheme is said to be fully homomorphic when it is possible to perform implicit addition and multiplication of plaintext while manipulating only ciphertexts. The first construction of a fully homomorphic scheme was described by Gentry in [Didlaet al. 2008].
Gentry described a “somewhat homomorphic” scheme that supports a limited number of additions and multiplications on ciphertexts. This is because the ciphertext noise increases with every multiplication and must remain upper-bounded; therefore only a polynomial of small degree can be applied on ciphertexts.

The second step in Gentry's framework consists in “squashing” the decryption procedure so that it can be expressed as a low degree polynomial in the bits of the ciphertext and the secret key. Then Gentry's key idea consists in evaluating this decryption polynomial not on the bits of the ciphertext and the secret-key (which would give the plaintext), but homomorphically on the encryption of those bits, which gives another ciphertext for the same plaintext. If the degree of the decryption polynomial is small enough, the noise of the new ciphertext can be actually smaller than in the original ciphertext, and therefore this new ciphertext can be used again in some homomorphic operation (either addition or multiplication). Using this “ciphertext refresh” procedure the number of permissible homomorphic operations becomes unlimited and one gets a fully homomorphic encryption scheme.

Gentry's original scheme [Didla et al. 2008], based on ideal lattices. Gentry and Halevi described in [Szczechowiak et al. 2009] the first implementation of Gentry's scheme, using many clever optimizations, including some suggested in a previous work by Smart and Vercauteren [Lee & Choi, 2006]. For their most secure setting (claiming 72 bits of security) the authors report a public key size of 2.3 GB and a ciphertext refresh procedure taking 30 minutes on a high-end workstation.

Van Dijk, Gentry, Halevi and Vaikuntanathan's (DGHV) have developed a scheme over the integers [De et al. 2003]. The scheme is conceptually simpler than Gentry's scheme, because it operates on integers instead of ideal lattices. Recently it was shown in [Ray et al., 2005] how to reduce the public-key size by storing only a small subset of the original public key and generating the full public key by combining the elements in the small subset multiplicatively. Using some of the optimizations from [Szczechowiak et al. 2009], the authors of [Ray et al. 2005] report similar performances: a 802 MB public-key and a ciphertext refresh of 14 minutes.
Brakerski and Vaikuntanathan's scheme is based on the Learning with Errors (LWE) problem [Abdelzaher et al. 2004; Zhou et al. 1999]. The authors introduce a new dimension reduction technique and a new modulus switching technique to shorten the ciphertext and reduce the decryption complexity. A partial implementation is described in [Koblitz, 1987], without the fully homomorphic capability.

Recently Brakerski, Gentry and Vaikuntanathan have published an amazing new framework [Sun et al. 2007] to better manage the ciphertext noise when evaluating a circuit homomorphically, using the dimension reduction technique and modulus switching technique from [Abdelzaher et al. 2004]. Under this new framework, the ciphertext noise increases only linearly with the multiplicative level, instead of increasing exponentially. This has the potential to significantly improve the practical performance of fully homomorphic encryption.

Jean-Sébastien Cor, et al. describe a compression technique that reduces the public-key size of the van Dijk et al.'s. fully-homomorphic scheme over the integers. This remains semantically secure, but in the random oracle model. A similar compression technique is also applicable to Brakerski and Vaikuntanathan's fully homomorphic scheme. The ways to adapt the new framework from Brakerski, Gentry and Vaikuntanathan for leveled fully homomorphic encryption to the van Dijk et al. scheme over the integers is also discussed.

In a discussion thread on the cypherpunks mailing list from 2000, Bram Cohen proposed a public key encryption scheme [De et al. 2003] that is quite similar to the scheme above. Secondly, in 2008, Levieil and Naccache applied the same general technique to construct what they called an “Insecure and Clumsy” Cryptographic Test Correction scheme, and used the additive homomorphic properties of the scheme to prevent students from cheating on their exams [Rivest et al. 1978]. Both these works appeared prior to the breakthrough result of Gentry in 2009 that showed the first fully homomorphic encryption scheme, and as such, do not observe or utilize the multiplicative homomorphism that the scheme could support.

The two main distinctions of the current work are

1. First, the security analysis in these prior works was informal, and concrete parameters were either not set, or set to trivially breakable values. The scheme in [Rivest et al. 1978] is trivially broken when considered as a cryptographic scheme, irrespective of
the choice of parameters. This is justified in their case since the adversary model they considered is very weak. In fact, prior to our work there was widespread belief in the cryptographic community that schemes of this form are inherently insecure. Hence, one of the contributions of this work is to point out that with an appropriate choice of parameters, this simple scheme can be made to resist all known attacks.

2. Second, and more importantly, neither of the works mentioned above even considered multiplicative homomorphism, and specific instantiations (when given) did not support even a single multiplication. Thus, another contribution of this work is to observe that not only can this scheme made to support multiplications, but it can be used within Gentry’s blueprint to construct a fully homomorphic encryption scheme.

3. Finally, a search-to-decision reduction is discussed, which shows that the semantic security of the scheme can be based on a well-defined search problem, namely the approximate GCD problem.

Regev’s first encryption scheme [Wang et al. 2008] is based on the unique shortest vector problem. It describes a very simple “somewhat homomorphic” encryption scheme using only elementary modular arithmetic, and use Gentry’s techniques to convert it into a fully homomorphic scheme.

Secret sharing was invented by both Adi Shamir and George Blakley, independent of each other, in 1979. Various secret sharing schemes are described below:

2.10 SECRET SHARING

2.10.1 Shamir's scheme [Shamir, A 1979]

In this scheme, any $t$ out of $n$ shares may be used to recover the secret. The system relies on the idea that we can fit a unique polynomial of degree $(t-1)$ to any set of $t$ points that lie on the polynomial. It takes two points to define a straight line, three points to fully define a quadratic, four points to define a cubic curve, and so on. That is it takes $t$ points to define a polynomial of degree $t-1$. The method is to create a polynomial of degree $t-1$ with the secret as the first coefficient and the remaining coefficients picked at random. Next find $n$ points on the curve and give one to each of the players. When at least $t$ out of the $n$ players reveal their
points, there is sufficient information to fit a \((t-1)\)th degree polynomial to them, the first coefficient being the secret.

2.10.2 Blakley's scheme [Blakley et al, 1994]

Two nonparallel lines in the same plane intersect at exactly one point. Three "nonparallel" planes in space intersect at exactly one point. More generally, any \(n\) nonparallel \(n\)-dimensional hyperplanes intersect at a specific point. The secret may be encoded as any single coordinate of the point of intersection. If the secret is encoded using all the coordinates, even if they are random, then an insider (someone in possession of one or more of the \(n\)-dimensional hyperplanes) gains information about the secret since he knows it must lie on his plane. If an insider can gain any more knowledge about the secret than an outsider can, then the system no longer has information theoretic security. If only one of the \(n\) coordinates is used, then the insider knows no more than an outsider (i.e., that the secret must lie on the \(x\)-axis for a 2-dimensional system). Each player is given enough information to define a hyperplane; the secret is recovered by calculating the planes' point of intersection and then taking a specified coordinate of that intersection.

Blakley's scheme is less space-efficient than Shamir's; while Shamir's shares are each only as large as the original secret, Blakley's shares are \(t\) times larger, where \(t\) is the threshold number of players. Blakley's scheme can be tightened by adding restrictions on which planes are usable as shares. The resulting scheme is equivalent to Shamir's polynomial system.

2.10.3 Secret Sharing using the Chinese Remainder Theorem

The Chinese Remainder Theorem can also be used in secret sharing, for it provides us with a method to uniquely determine a number \(S\) modulo \(k\) many relatively prime integers. There are two secret sharing schemes that make use of the Chinese Remainder Theorem, Mignotte's and Asmuth-Bloom's Schemes. They are threshold secret sharing schemes, in which the shares are generated by reduction modulo the integers, and the secret is recovered by essentially solving the system of congruencies using the Chinese Remainder Theorem.
2.10.4 Proactive secret sharing

If the players store their shares on insecure computer servers, an attacker could crack in and steal the shares. If it is not practical to change the secret, the uncompromised (Shamir-style) shares can be renewed. The dealer generates a new random polynomial with constant term zero and calculates for each remaining player a new ordered pair, where the x-coordinates of the old and new pairs are the same. Each player then adds the old and new y-coordinates to each other and keeps the result as the new y-coordinate of the secret.

All of the non-updated shares, the attacker accumulated, become useless. An attacker can only recover the secret if he can find enough of other non-updated shares to reach the threshold. This situation should not happen because the players deleted their old shares. Additionally, an attacker cannot recover any information about the original secret from the update files because they contain only random information. The dealer can change the threshold number while distributing updates, but must always remain vigilant of players keeping expired shares.

2.10.5 Verifiable secret sharing

A player might lie about his own share to gain access to other shares. A verifiable secret sharingscheme allows players to be certain that no other players are lying about the contents of their shares, up to a reasonable probability of error. Such schemes cannot be computed conventionally; the players must collectively add and multiply numbers without any individual's knowing what exactly is being added and multiplied. Tal Rabin and Michael Ben-Or devised a multiparty computing system that allows players to detect dishonesty on the part of the dealer or on part of up to one third of the threshold number of players, even if those players are coordinated by an "adaptive" attacker who can change strategies in realtime depending on what information has been revealed.

2.10.6 Computationally Secure Secret Sharing

The disadvantage of unconditionally secure secret sharing schemes is that the storage and transmission of the shares requires an amount of storage and bandwidth resources equivalent to the size of the secret times the number of shares. If the size of the secret were significant, say 1 GB, and the number of shares were 10, then 10 GB of data must be stored by
the shareholders. Alternate techniques have been proposed for greatly increasing the efficiency of secret sharing schemes, by giving up the requirement of unconditional security.

One of these techniques, known as secret sharing made short,[Abdelzaher et al. 2004] combines Rabin's information dispersal algorithm[Zhou et al. 1999](IDA) with Shamir's secret sharing. Data is first encrypted with a randomly generated key, using a symmetric encryption algorithm. Next this data is split into N pieces using Rabin's IDA. For example, if the threshold were 10, and the number of IDA-produced fragments were 15, the total size of all the fragments would be (15/10) or 1.5 times the size of the original input. In this case, this scheme is 10 times more efficient than if Shamir's scheme had been applied directly on the data. The final step in secret sharing made short is to use Shamir secret sharing to produce shares of the randomly generated symmetric key (which is typically on the order of 16 - 32 bytes) and then give one share and one fragment to each shareholder. A related approach, known as AONT-RS,[Ray et al. 2005] applies an All-or-nothing transform to the data as a pre-processing step to an IDA. The All-or-nothing transform guarantees that any number of shares less than the threshold is insufficient to decrypt the data.

**Table 2.2 Summary of various security schemes for wireless sensor networks**

<table>
<thead>
<tr>
<th>Security schemes</th>
<th>Attacks Detrred</th>
<th>Network Architecture</th>
<th>Major Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Worm hole based[David R, et al., 2007]</td>
<td>Dos Attack(jamming)</td>
<td>Hybrid (mainly wireless partly wired) sensor network</td>
<td>Uses wormholes to avoiding jamming.</td>
</tr>
<tr>
<td>Statistical En-Route Filtering[Frank Stajano, et al., 2002]</td>
<td>Information spoofing</td>
<td>Large No. of Sensors. Highly Dense WSN.</td>
<td>Detects and drops false reports during forwarding process.</td>
</tr>
<tr>
<td>Attack Type</td>
<td>Description</td>
<td>Traditional Wireless Sensor Network</td>
<td>Remarks</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------</td>
<td>--------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Bidirectional Verifications</td>
<td>Hello Flood Attack</td>
<td>Traditional wireless sensor network</td>
<td>Adopts probabilistic secret sharing. Uses bidirectional verification and multi-path multi-base station routing.</td>
</tr>
<tr>
<td>TIK</td>
<td>Wormhole Attack, Information or Data Spoofing.</td>
<td>Traditional wireless sensor network</td>
<td>Based on symmetric cryptography. Requires accurate time synchronization between all communicating parties, implements temporal beaches.</td>
</tr>
<tr>
<td>Random Key Predistribution</td>
<td>Data and information spoofing. Attacks in information in Transit.</td>
<td>Traditional wireless sensor network</td>
<td>Provide resilience of the network. Protect the network even if part of the network is compromised, Provide authentication measures for sensor nodes.</td>
</tr>
<tr>
<td>REWARD</td>
<td>Blackhole attacks</td>
<td>Traditional wireless sensor network.</td>
<td>Uses geographic routing. Takes advantage of the broadcast inter-radio behavior to watch neighbor transmissions and detect blackhole attacks.</td>
</tr>
<tr>
<td>Tiny See</td>
<td>Data and Information spoofing. Message Replay Attack.</td>
<td>Traditional wireless sensor network.</td>
<td>Focus on providing message authenticity, integrity confidentiality. Works in the link layer.</td>
</tr>
</tbody>
</table>