Monograms
On
Issues and Challenges in Wireless Sensor Networks
Vimal Kumar

Express progress in the field of technology made it feasible to foster wireless sensor networks technology [1]. Wireless Sensor Networks (WSN's) are comprised of large number of tiny sensor nodes with constrained resources in terms of processing power, energy and storage. WSN can be used in various applications mainly environmental monitoring, medical, military, and agriculture [1]. Since, devices used in sensor networks are not tamper resistant, so adversary can gain its physical access easily. Hence, the main objective is to protect the data from unauthorized access, which can be done by using some security mechanisms [6-9]. The technology faces lots of security problems as it has a wireless mode of communication and access to such sensor devices is quite easy. There are two approaches to restrict the unauthorized access in to the network: symmetric cryptography and asymmetric cryptography.

In traditional Public Key Infrastructure (PKI), the user selects a public key but it needs to be validated by a trusted third party known as Certificate Authority (CA) [3]. The CA provides a digital certificate to tag the public key with the user's identity. PKI has a problem of high computation and storage. To avoid this, Shamir introduced the concept of Identity-based Infrastructure. It allows the user to choose a public key of its own choice such as email-id, phone number, name, etc. and the private key is generated by trusted third party server. Many researchers are using bilinear pairing assumption to construct a certificate-less signature [7]. But the problem with these bilinear pairing techniques is that implementation of pairing is way harder than RSA based implementations. Building an inefficient prototype implementation of pairings is far from straightforward for anyone but an expert, and even then it is often difficult or impossible to generate curves with the desired security parameters. As we know that RSA technique has been applied in different atmospheres for decades. Jianhong Zang et al. [6] proposed a RSA based certificate-less scheme under Strong RSA and Discrete Logarithm problem.

Drawback of this scheme was that it was not secure under Type I attack if we provide enough power to the attacker.

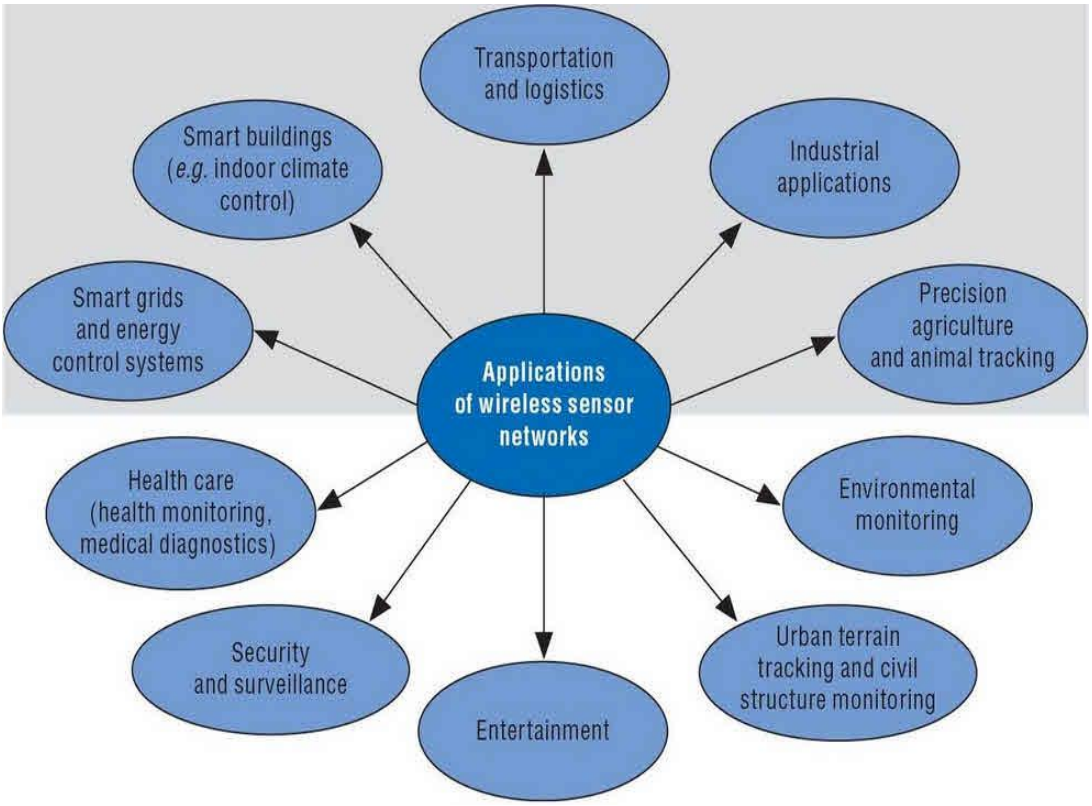

Fig. 1: Applications of WSN's

Two main responsibility of WSN are data aggregation and communication between CHs and base stations [4]. Among all the challenges like low energy of sensors and network life time, security during the different transmission phases of WSN is a prior challenge. Communication medium in WSNs is unprotected and untrusted because of limited resources and broadcasted and self-organized transmission medium. Most security techniques used in other networks are not sufficient for wireless sensor networks and security is a vital issue in any network [3]. Providing security in wireless sensor network is very critical due to following challenges:

- **Achieving Confidentiality** Due to limited energy implanted in sensors and wireless medium applying cryptography and encryption techniques is bit challenging. However due to data redundancy and aggregation property of sensor network, compromise of some sensor node would not be a total security loss.

- **Ad hoc deployment** means no fixed structure of sensor network, which means nodes are self-organized and mobile. So security scheme must be able to operate in different dynamic environment and in situations like node failure, new node addition etc.
- **Timing beclouding** during the transmission of information timing and location of communication are very important concerns for intruders to eavesdrop. So to identify cost-effective schemes for hiding the timing information in sensor networks is a big challenge.
- **Topology beclouding** unlike traditional networks, sensor networks perform aggregation on data before sending it to base station. So nodes near to base station are having more valuable information than away nodes. If attacker compromises a node which is near to BS, it would be more harmful to network. So it's a challenge to hide the routing infrastructure of the sensor network.
- **Hostile environment** when a sensor network is deployed in a hostile area, one can physically damage the sensor node and gain access to it. These hostile situations represent major challenge in a way of security and network damage as well for researchers.
- **Immense Scalable trust management** trust management means to find nodes in sensor network which are legitimate and which are untrusted. Developing algorithms to do such task in a large scale network is very challenging because of physical compromise, limited energy and resources and frequent requirement of re-establishing the trust management.
- **Secure aggregation** As aggregation takes place at intermediate nodes in sensor network, end to end encryption and decryption to base station is not possible. So developing a cryptographic approach for secure data aggregation is very challenging.

1.1 SECURITY REQUIREMENTS FOR SENSOR NETWORKS

Main requirement of security is to ensure safe and trusted transmission of data between nodes and base station in sensor network. Researchers are developing different cryptographic approaches to achieve following goals for security [5]. Security of a wireless sensor network can be divided in 2 major categories:

- Operational security of WSN's
- Information security

In the operational related security, our main objective is that a wireless sensor network, as a whole, should continue to perform properly even if some of its components are under attack. This also known as service availability requirement of a sensor network.

The information based security is based on the fact that *confidential* information provided by the sensor node should never be disclosed. Apart from *confidentiality* a sensor network should always be assured of achieving the *integrity*, *authentication* and *non-repudiation* also. In different applications domain of wireless WSN's, there exists lots of requirements of security for sensor network [23]. For different application scenarios of wireless sensor networks, in Table 1 we have described possible violated security properties below. These are as follows:

Table 1: Security Threads and Violations in Different Application of WSN's

Application Domain	**Possible Potential Securitythreats**	**Violation of Properties**				
		S	**C**	**I**	**A**	**N**
Military	Eavesdropping of classified information		Y			Y
	Denial-of-service attacks	Y		Y		
	Supply of corrupted or misleading information				Y	Y
Environmental Monitoring	Monitoring of any Factory fuel emission and its radiation by government and factory may cause modification in original data.			Y		Y
Hospital	Providing wrong information about the current condition of different organs of a patient body to career or doctor, this may cause potentially fatal diagnosis and alter the treatment which could be performed on patient.			Y	Y	

Intelligent Building	One can compromise the Token-based access control mechanisms if used token authentication protocol could be compromised.				Y	Y
	One can pass the Biometrics-based access control if he can fool or pass the biometric sensor.	Y		Y	Y	
Space exploration	The projects for exploring the space needs to be most secure because they run in real time environment because they want all commands to run logically on their space.	Y	Y	Y	Y	Y
Transportation	One can easily spoof the traffic control and it could be major flaw of order to be in a city.			Y	Y	
Disaster Detection	Supply of misleading information				Y	Y
Industry	Eavesdropping of commercial secrets by business rivals.		Y			
	One can intentionally corrupt the manufacturing of any item which may lead to the misleading reading of sensors.			Y		Y

S- Service availability, C- confidentiality, I- integrity, A- authentication, N- non- repudiation

1.1.1 SECURITY GOALS

From the table 1.1 we can observe that to successful performance of wireless sensor depends on these security goals given below.

- **Confidentiality**

Data confidentiality is ability to secure a message from third party like a passive attacker. That means communication between two sensor nodes should be confidential. This is most basic goal of network security. Confidentiality is an assurance of authorized access to information. The objective of confidentiality in a wireless sensor environment is to protect the communicative data between sensor nodes or between sensor nodes and the base station from being disclosed, because an adversary having right amount of information and equipment can eavesdrop on information. So in case of wireless sensor networks data confidentiality is defined as following: [42] [43]

1. A sensor node in network must not leak readings of itself to its neighbor sensor nodes. This should be most accurate in case of military environment sensor network, therefore to secure the highly sensitive information data confidentiality is very important and necessary.
2. There are number of application where nodes communicate very sensitive data like key distribution, therefore confidentiality is necessary.

- **Authentication**

This ensures the receiver that data is coming from a trusted and claimed source and also for source that packet is going to a claimed destination. In a wireless network environment an adversary can easily implant a fake message to network, so receiver needs to be aware that message is coming from an authenticated source.

There could be a case in wireless sensor network where an adversary can claim as legitimate receiver also, so there should also be an authentication on sender side also that he/she is sending the message to a legitimate destination.

- **Integrity**

Integrity in sensor network is ability to ensure that message during transmission is not modified or tempered. There may be a case that integrity of network be compromised even if confidentiality and authentication is ensured.

- **Non-repudiation**

This proves that particular data packet came from a particular source. During the authentication source proves that its identity is right. Non-repudiation ensures that source cannot deny that it sent a packet.

- **Data Freshness**

Although if confidentiality and integrity of data is ensured, it is important to manage data freshness in network. This ensures that data sent is fresh and no old messages are resent again in transmission. Importance of data freshness increases if there is an environment where shared key strategies are used in the design. As we know that in these designs we need to change shared keys over time. However, propagation of keys in network is time consuming process. So during this time an adversary can use replay attack.

1.1.2 ATTACKS IN WSN's

Wireless Sensor Networks are very vulnerable for different types of attacks because of their unsafe environment. These attacks in sensor networks could be either active attacks or of passive attacks, active attacks like denial of service attacks, modification, fabrication, routing attacks like spoofing, Sybil attack, blackhole attack and wormhole attacks and passive attacks like traffic-analysis, privacy invasion, physical-attacks, eavesdropping and so on.

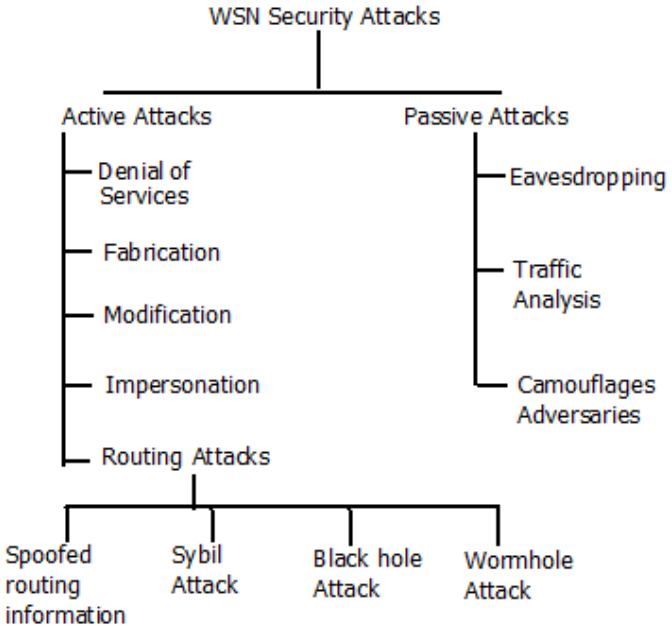

Fig. 1: Taxonomy of WSN Security Attacks

To guard a wireless sensor network from a well-orchestrated attacks of denial of service is near to impossible because of asymmetric power potentials and computational constraints. If there is node with more power, then it can jam the working of a sensor node and also prevent a node from performing its basic intended duties. Here we will discuss some of these attacks.

- **Denial of Service Attacks**

A simple way to attack the wireless sensor network is to jam a sensor node or set of sensor nodes and prevent them from performing the intended task of that node. Jamming, for this case, is just transmitting the radio signals which are found to be in interferes with the radio frequencies which being used by the sensor network [6]. There are 2 types of signal jamming which are constant jamming and intermittent jamming. In case of constant jamming, complete network is jammed and there are message which are able to receive or sent. If jamming is of intermittent type, nodes in network can exchange the messages in periodic manner but not in consistent manner [6].

- **The Sybil attack**

Newsome et al. described the Sybil attack which relates to wireless sensor networks [45]. We can simply define the Sybil attack as an attack which could be able to defeat the redundancy mechanisms of distributed data storage systems in peer-to-peer networks. During the Sybil attack a malicious/adversary node takes the identity of different sensor nodes and effects the routing information of multiple nodes by a single malicious node.

- **Traffic Analysis Attacks**

In a typical wireless sensor network lots of low power contained sensors communicate with each other as well as powerful and robust base station. It is not strange, in this manner, for information to be accumulated by the individual nodes where it is eventually directed to the base station. Frequently, for an adversary to viably render the network pointless, the adversary can just cripple the BS. Deng et al. [46] showed two attacks that can distinguish the BS in a network (having more probability) without notwithstanding comprehension the substance of the packets (if the packets are themselves scrambled) A rate observing assault essentially makes utilization of the thought that hubs nearest to the base station tend to forward a larger number of packets than those more

distant away from the base station. An attacker require just screen which nodes are transmitting the packets and take after those sensor nodes which sends largest amount of packets [46].

- **Physical Attacks**

Sensor networks normally work in threatening open air situations. In such situations, the little frame element of the sensors, combined with the unattended and appropriated nature of their organization make them exceedingly defenseless to physical assaults, i.e., dangers because of physical node devastations. Not at all like numerous different assaults said above, physical assaults annihilate sensors for all time, so the losses are irreversible.

1.2 PUBLIC KEY CRYPTOGRAPHYAND RSA

Typical public key cryptosystem contains a pair of different keys which are associated with each other. One key is known as public key which is known to all, so released publically while other is known as private key, and known only to the owner of key. Private Key is designed, computationally not possible to calculate by using the public key. A typical public key encryption system has 6 ingredients.

- **Plaintext:** can be indicated as a readable message which is used as input when initializing the algorithm.
- **Cipher text:** This is the encrypted message which is produced as output. Output of plaintext depends on the plaintext and the key used in encryption algorithm. For a given message, cipher texts produced by two (public and private) keys will be different.
- **Public key:** Public key is defined as key known publically to all in that network. Anyone in that network can access and make use of that key for either encryption or decryption.
- **Private Key:** Private Key is only known to the owner of that key and can be used by owner only to encrypt or decrypt ant message.
- **Encryption Algorithm:** Different transformation on plaintext could be performed by using an appropriate encryption algorithm.
- **Decryption Algorithm:** This algorithm receives the cipher text as input and by using the associated matching key produce plaintext as output for this algorithm.

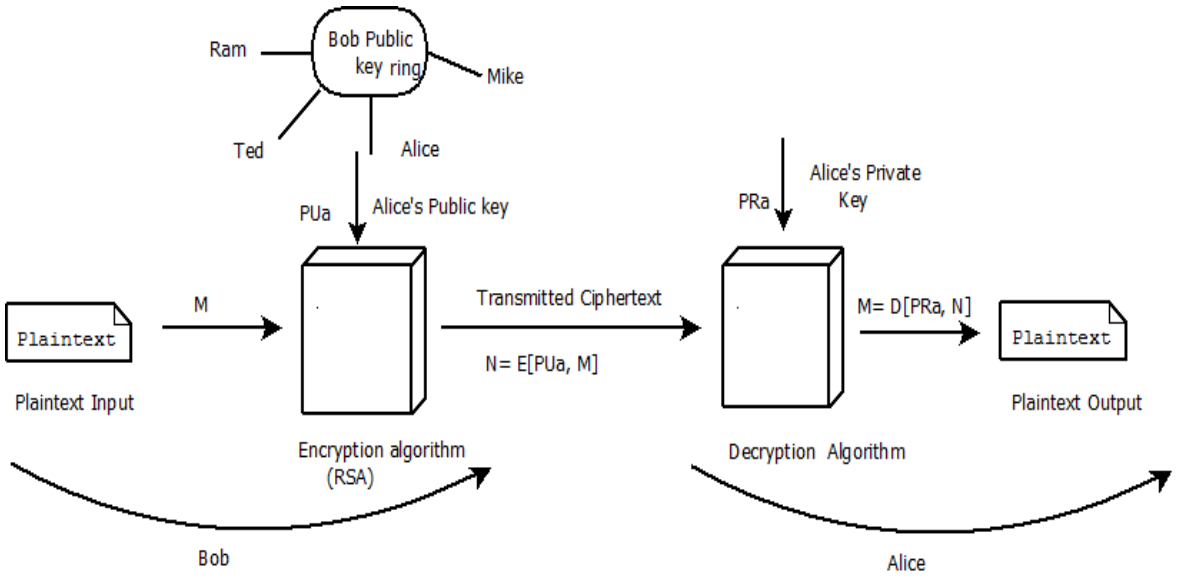

Fig. 3: Encryption with Public key in PKC

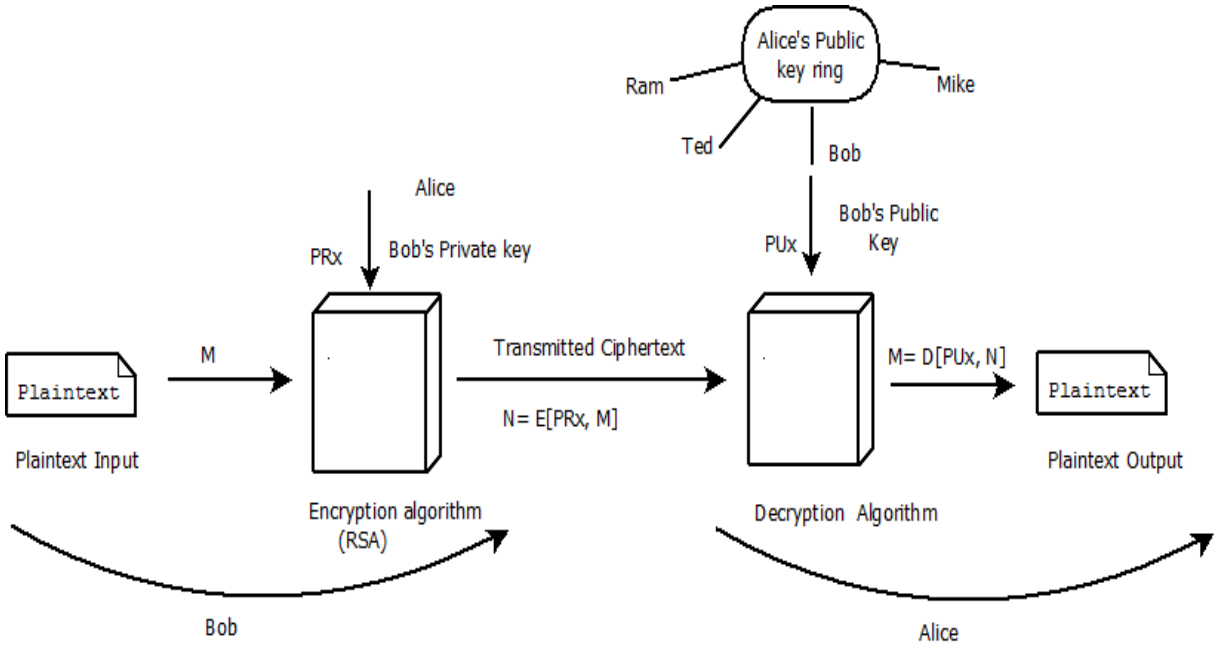

Fig.4: Encryption with Private Key in PKC

So public key cryptosystem has broad application area. Table 2 shows some real application being used in different algorithms.

Table 2: Applications of Public Key Cryptosystem

Algorithms	Encryption/Decryption	Key Exchange	Digital signatures
RSA	Yes	Yes	Yes
Elliptic Curve	Yes	Yes	Yes
Diffie- Hellman	No	Yes	No
DSS	No	No	Yes

1.2.1 RSA CRYPTOSYSTEM

In 1978 Ron Rivest, Shamir and Adleman invented an ID based public key infrastructure based cryptosystem whose theoretical facts were based on Eular'steorem. They named their encryption system RSA Cryptosystem. This is one of the most used and common system to encrypt data today. RSA algorithm can be described as follows:

- Select 2 distinct large prime numbers p and q.
- Define $n = pq$.
- Find *Euler's phi function* $\phi(n) = (p-1)(q-1)$.
- Select an integer e such that it will be relatively prime to $(p-1)(q-1)$.
  So e satisfies $\gcd(e,\ \phi(n)) = 1$.
- Calculate a positive integer d which satisfies
  $$ed \equiv 1\ mod\ ((p-1)(q-1)).$$
- For a input message M which we want to encrypt, the message is encrypted as
  $$E = M^e\ mod\ n$$
- For receiving the message M from encrypted message
  $$M = E^d\ mod\ n$$

So we can see that in RSA cryptosystem, message is encrypted by e (public key) and for decryption we use d (private key).

1.3 RANDOM ORACLES MODEL

In modern cryptography, proofs of security schemes are often relative to the computational hardness of some well-known mathematical problems which are hard to solve. So for an efficient functionality of scheme to work well, it is necessary to use an idealized model. Random Oracle Model is a well-known computational model for giving proof about the security of a cryptography scheme. This model was formalized by Bellare and Rogaway [22] in 1993. In Random Oracle Model a given hash function is replaced by publically accessed random oracle which is also known as theoretical Black Box to analyze the security scheme. This random oracle gives response (True) to each unique query from a fixed output domain randomly. There are some artificial signature schemes which are proved secure in random oracles and these schemes are trivially not secure in real world environments. Nonetheless, for a more natural signature cryptography protocol the proof of security in Random Oracle Model is a strong indication of practical security proof of protocol.

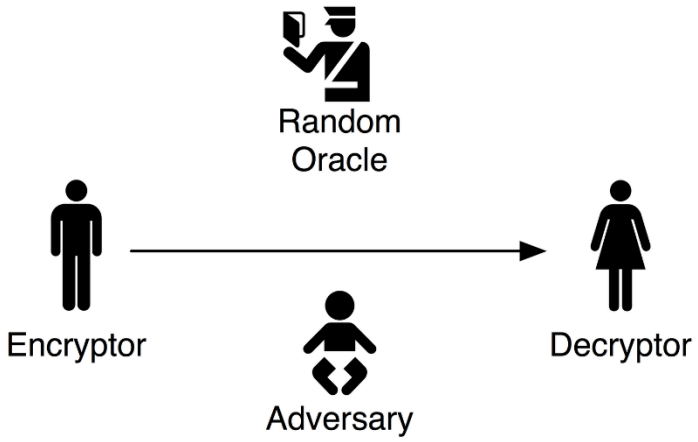

Fig 1.5: Typical Random Oracles Model

As a preliminary to proof the security of our RSA based certificate-less signature scheme, we are going to use Discrete Logarithm Problem for our security algorithm.

1.4 MOTIVATION

During this era as the technology is growing very fast, wireless sensor networks could be widely used in different needs like environmental monitoring, military areas, hospitals, home monitoring etc. As these networks are wireless, this makes them very venerable to be intruded. So providing security to these networks from different types of attacks and ensuring integrity of communication, authentication of sensor nodes is very important. Researchers have already proposed different security schemes like public key cryptography, cryptography using a certificate, ID based signature schemes and other many techniques. Recently Zaho has proposed a RSA based certificate-less signature scheme which is lot more efficient than other available techniques which we can actually implement in real life applications. But in 2012 Debiao He et al. showed that Zaho's scheme is not secure under Type I attacks.

2. BACKGROUND AND LITERATURE REVIEW

2.1 Algebra And Number Theory

In modern cryptography, role of algebra and number theory is very important. Most public key cryptography systems and protocols are based on the theorems and algorithms of algebra and number theory. This section on dissertation is focused on studying some well-known results of number theory and algebra.

2.1.1 Integer Arithmetic

Let $\mathbb{Z}$ denotes a set of integers $\{\dots\dots, -4, -3, -2, -1, 0, 1, 2, 3, \dots\}$ and $\mathbb{N} = \{n \in \mathbb{Z} | n \geq 1\}$ represents a set of natural numbers. Suppose $a, b \in \mathbb{Z}, and\ a \neq 0$. Then we can divide b by a having remainder *r.* So on this basis the Fundamental Theorems of Arithmetic are defined below:

Theorem 2.1.1 (Fundamental Theorem of Arithmetic):"$Let\ n \in \mathbb{N}, n \geq 2. there\ exists\ \ distinct\ primes (pairwise)\ p_1, \dots\dots, p_k\ and\ exponent\ e_1, \dots\dots, e_k \in \mathbb{N}, e_i > 0, i = 1, 2, \dots k$ " such that,

$$n = \prod_{i=1}^{k} {p_i}^{e_i}$$

Where $\mathbb{N}$ is set of natural numbers and $primes\ (p_1, \dots\dots, p_k)\ and\ exponents\ (e_1, \dots\dots, e_k)$ are unique.There also exists some efficient algorithms for addition, multiplication, subtraction and division of natural numbers.

Theorem 2.1.2 (The Euclidean Algorithm):"Suppose a, b ∈ ℤ (b ≥ a > 0),*and setb* = r_{-1} *and* $a = r_0$.*After applying the division algorithm repeatedly, we get*$r_{j-1} = r_j q_{j+1} + r_{j+1}$ with $0 < r_{j+1} < r_j$ for all $0 \leq j < n$, *where n is the smallest nonnegative number such that*$r_{n+1} = 0$, *in which case* $\gcd(a, b) = r_n$."

2.1.2 Basic Algebra

Let S is a non-empty set. We define a binary operation * on set S, which is a mapping from $S \times S$to S. If $a, b \in S$ then $a * b$ denotes the result of * applied on a *and* b. If there exists a condition that $a * (b * c) = (a * b) * c$ for all $a, c, b \in S$, then * operation is said to be associative operation and if $a * b = b * a$, then operation is known commutative. If there exists an element $e \in S$ such that $* a = a * e = a \; for \; all \; a \in S$, then e is said to be identity element of set S.An element $b \in S$ is said to be inverse of an element $a \in S$if $a * b = b * a = e$. Where $e$can be said identity element for a.

Groups

Definition 2.1.3 (Group): *LetGbe a non-empty set and * is defined as binary operation on G, then the pair $(G,*)$ is said to be a group if*

1. *Operation * is associative on G i.e.* $a * (b * c) = (a * b) * c$ *for all* $a, c, b \in S$
2. *G contain an identity element* $e \in S$ *such that* $e * a = a * e = a \; for \; all \; a \in S$
3. *G contain an inverse element* $b \in S$ *such that*$a * b = b * a = e for \; all \; a \in S$

We can call a group$(G,*)$*abelian or commutative if*$a * b = b * a$*for all*$a, b \in S$*.the order of a given group*$(G,*)$ is denoted as $|G|$.Some regularly used group definitions are defined as follows:

- $(\mathbb{Z}, +)$: "Where $\mathbb{Z}$ is non- empty set of all the integers and + is regular addition operation. Identity element of this group is 0 and inverse of an element $a \in \mathbb{Z}$is $-a$".
- $(\mathbb{Z}_n, +)$:"Where $\mathbb{Z}_n = \{0,1,2, \ldots . n-1\} \; and +$ is said congruent addition (addition modulo *n*), we can identify that identity element of this group is 0 and inverse of an element $a \in \mathbb{Z}$is $n-a$".

- $(\mathbb{Z}_n^*,*)$:"Where $\mathbb{Z}_n^* = \{a | a \in \mathbb{Z}_n, \gcd(a,n) = 1\}$ and $*$ is said to be congruent multiplication (modulo n). The identity element is defined 1, and inverse of element a can be computedby using the extended version of Euclidean algorithm".

Definition 2.1.4 (Cyclic Group):"*A Group G is said to be cyclic group if there exists a $g \in G$ such that each element $a \in G$ can be calculated as g^x for some $x \in \mathbb{Z}$. So we can say that $= \{g^i | i \geq 0\}$. theng is called as generator of group and written as $\langle g \rangle = G$*".

Definition 2.1.5 (Sub Group):*"let $(G,*)$ be a group. Then we can state that $(H,*)$ will be known as a subgroup of $(G,*)$, if $H \subseteq G$ and $(H,*)$ is already a group."*

For example:

If $(G,*)$ be a group. Then for any $a \in G$, if $\langle a \rangle = \{g^i | i \geq 0\}$ exists, then a will be a subgroup of G.

2.2 EULER's THEOREM

To understand the Euler's Theorem first we need to discuss Lagrange's Theorem.

Theorem 2.2.1 (Lagrange's Theorem): *"Let $(G,*)$ be a finite group and $(H,*)$ is a subgroup ofgroup$(G,*)$. Then $|H|$ $divides |G|$."*

Proof: Proof of this theorem can be easily performed by showing that every coset of G has $|H|$ elements. So if we prove that $|H| = |Ha|$, then this is sufficient to prove the theorem. This can be done by applying the 1-1 onto function between $|H|$ and $|Ha|$.

Corollary 2.2.2: *Suppose G be a finite group with $n = |G|$. If $a \in G$, then $a^n = e$.*

Theorem 2.2.3 (Euler's Theorem): if we take a special case for corollary 2.2.2 we can state the Euler's Theorem as follows:

Let n is a positive integer and $n \in \mathbb{N}$. If a be an integer with $gcd(a,n) = 1$, then we can obtain that $a^{\phi(n)} \equiv 1 \, mod \, n$.

Proof: given that $gcd(a,n) = 1$. We can say that $\bar{a} \in \mathbb{Z}_n^*$, a group of order $\phi(n)$.As stated in corollary 2.2.2 we can identify that $\bar{a}^{\phi(n)} = \bar{1}$. By the definition of coset multiplication, $\bar{a}^{\phi(n)} = \overline{a^{\phi(n)}}$. So we can state that equation $\bar{a}^{\phi(n)} = \bar{1}$ can be written as $a^{\phi(n)} \equiv 1 \, mod \, n$.

Theorem 2.2.4(Forking Lemma): In case of a cryptosystem, this lemma states that "*If there is an adversary (basically probabilistic Turing machine), on input from any distribution, generates an output which contains some properties with non-negligible probability, then with the same probability, if same adversary again runs on some new input but on the same random oracle tape, the resultant output will also have same properties as first output*."

The concept of forking lemma was firstly used by David Point cheval et al. [58] in "Security proofs for signature schemes" to prove the security of their scheme. After that in 2006 Gregory Neven et al. [59], generalized the concept of forking lemma.

2.3 PRIME NUMBER GENERATION

Algorithms who are using public key cryptosystem for encryption needs prime numbers to develop a secure key management system. A large size network needs lots of these primes.

In real world implementation of generation of prime number takes place as follows:

- Develop a $n - bit \, number \, p$ randomly.
- Set the bits of high order as well as of low order to 1. The high order 1 bit makes sure that generated prime number is of desired length and the low order 1 bit ensures that value is odd.
- Check by any small primes: 3, 5, 7, 11, and so on, to make sure that $p$is not divisible. The most desirable way is to test that $p$is divisible by all the prime numbers less than 2000 or not. This can be done efficiently by using a wheel [24].
- Perform the Rabin-Miller test on a random number a. if test is passed by p, perform another test with another random number a. perform at least 5 tests to be sure. If p fails, then choose another and repeat the above process.

Strong Primes: In public key cryptosystem, when we choose $n = pq$, the product of 2 prime numbers, then it is efficient and desirable that we use strong prime numbers for$p$ and q. These numbers are the prime numbers which have some properties that makes the product $n$difficult to factor by some specific factoring methods.

There are some suggestions to select strong primes [25-26].

- gcd $of\ Eualr's\ phi\ function\ ((p-1),(q-1))\ s$hould be small.
- $p-1$ and $q-1$, both should have large prime factors $p'\ and\ q'$respectively.
- Prime factors of $p'-1$ and $q'-1$ should be large.
- $p+1$and $q+1$, both should also have large factors of prime.
- $p = 2p'+1$and $q = 2q'+1$, where $p'\ and\ q'$ are relatively large prime numbers.

2.4 HASH FUNCTIONS

In ID based cryptography schemes Hash functions are used to restrict the integrity of a message. In digital signature algorithms, hash functions can be used to reduce messages of large (arbitrary) lengths into a message of given fixed length message which we can use in place of the original transmitted messages during signature generation. During the security proof of schemes by random oracles model, these hash functions are replaced by random oracles to perform different queries given by adversary. [27]

Definition 2.4.1 (Hash Function):"*A hash function can be defined as a function used to map a string if arbitrary finite length into a fixed length binary string of length l:"*

$$h: \{0,1\}^* \longrightarrow \{0,1\}^l$$

A hash function to be used in cryptosystem should be efficiently computable.

One Way Hash-Function:

For a one way hash function $H(M)$, if there is message/image of arbitrary length, then $H(M)$ returns a value of fixed length *h*, such that

$$h = H(M),$$

where, h is defined as a fixed length value for message M.

2.5 DISCRETE LOGARITHM PROBLEM (DLP)

Discrete logarithms in mathematics are logarithms which are defined with respect to multiplicative cyclic groups. Suppose *G* be a multiplicative cyclic group and $g \in G$ is a generator of *G*, then as in the definition given for cyclic groups, we know that for every element *y* of G, there exists a value g^x for some *x.* So x can be defined as discrete logarithm of *y* to the base g.

We can define discrete logarithm problem as follows: if there is a cyclic group $(G,*)$. If g is a generator of group*G* and there is an element such that$y \in G$, one's goal is to calculate the discrete logarithm of element *y* to the base g in the cyclic group *G*. Discrete logarithm problem is known as a NP – Hard problem. But this problem is not always defined as hard. The hardness of this problem depends on type of group selected.

To make discrete logarithm problem very hard to solve we need to take the modular of group to be a large prime number.

For example, when we need to choose a group for the crypto systems whose security proof is based on DLP, we use group Z_n^* where *n* is prime. However, if $n-1$ is a product of small prime numbers, then the algorithm given by Pohlig–Hellman is able to solve discrete logarithm problem very efficiently for this group. So to create a good crypto-system whose security is depend on discrete logarithm basis, the prime should be a safe prime.

As we discussed in upper section of this dissertation, we can say that a safe prime number is a strong prime which can be calculated as $2q+1$ where q is a large prime number. This guarantees that $n-1 = 2q$ which is an indication of strong prime number. So we can argue that Pohlig–Hellman

algorithm will not easily be able to solve DLP having strong prime number as modular of that cyclic group. To make an ID based cryptographic algorithm secure in random oracle n should be very large.

Discrete Logarithm Problem for RSA based signature: As given in the article above, we can define Discrete Logarithm Problem for our RSA based certificate-less signature scheme as follows:

"Suppose $n = pq$ is an RSA modular number which satisfy $p = 2p' + 1$, $q = 2q' + 1$ and $g \in Z_n^*$ where g represents as generator of order $p'q'$, for an element *y* in group *G,* one's goal is to generate the exponent *x* such that $y = g^x mod n$.

3.1 RELATED WORK

To provide security in wireless infrastructure-less medium researchers are using bilinear pairing techniques, public key cryptography, id based cryptography and other techniques [5, 6, 7, 9, 11]. Researchers presented lots of schemes for security using these techniques.

While studying the resource constrained wireless sensor networks, some [6] have focused specially on attacks and vulnerabilities in wireless sensor networks. Wood and Stankovic [6] surveyed a lots of denial of service attacks against WSNs, and discussed some possible solutions for these attacks. Karlof and Wagner [7] focused on routing layer attacks, and showed how some of the existing WSN protocols were vulnerable to these attacks. They provide valuable guidelines for proposal of our scheme. Since, the pairing operation is the most expensive operation, so researchers needed to find an alternative solution. In 2009, Wang et al. [20] proposed a scenario where pairing is not needed to be computed at sign phase, it precomputes and publishes as the system parameters. But, this is not the solution for the removal of pairing operation. In 2011, He et al. [18] developed an efficient short CLS scheme without pairing. After that some schemes were proposed based on analysis of Elliptic Curve Discrete Logarithm Problem [11, 21].

Deng et al. [46] showed two attacks that can distinguish the BS in a network (having greater probability) without notwithstanding comprehension the substance of the packets (if the packets are themselves scrambled) A rate observing assault essentially makes utilization of the thought that hubs nearest to the base station tend to forward a larger number of packets than those more

distant away from the base station. An attacker require just screen which nodes are sending packets and take after those sensor nodes which are sending largest amount of packets.

J. P. Walters et al. [51] surveyed different scenarios ragarding the security of wireless sensor networks. In this paper they present the hindrances and the necessities in the sensor security, arrange a hefty portion of the present attack on wireless sensor networks, lastly list their comparing different defensive measures.characterize the fundamental parts of remote sensor network security into four real classifications: the deterrents to sensor network security, the necessities of a safe wireless sensor network, assaults, and cautious measures. They discussed different obstacles regarding the security of WSN's like limited memory and power space, unreliable communications like conflicts and latency, unattended operatons like exposer to the physical attacks and so on. They also berifly discussed the different defensive measures like key establishment, secure broadcastiong, secure data aggregation, intrusion detection techniques for wireless sensor networks, reaching security againest physical attacks, trust management and much more.

One kind of AKE protocols [52,53] that has gotten noteworthy consideration as of late is the one outlined with passwords. It permits correspondence gatherings to build up validated session key for using so as to ensure secure interchanges just short secret passwords that possess little memory space and encourage person's recollecting. As a result of the effortlessness and accommodation of the method, it is especially alluring for the useful situations in which correspondence gatherings are lightweight or are handheld gadgets (portable PC and cell phone) that can't manage the cost of heavyweight security framework, for example, open key infrastructure.Related takes a shot at watchword validated group key exchange schemes for a MANET and WSN's incorporate.

Some of wireless sensor network security protocols [54–56] have concentrated on an AKE utilizing a mutual secret word among customers or between a customer and a server. Then again, it is clear that such a setting, to the point that all customers have the same watchword is not down to earth on the grounds that a secret key shouldn't be a typical mystery but rather ought to be a mystery of a person. For instance, in mission-discriminating MANETs, for example, those utilized in crisis salvage operations, the setting in which assemble portable hubs have distinctive passwords is more suitable.

Al Riyami et al. [2] proposed the first CL-PKC (Certificate-less public key cryptography) scheme. They described a scheme which use public key cryptography technique but do not require the

certificate to generate public key and to encrypt data. They make use of a new key generation environment which they named KGC (key generation center). They used the KGC to generate the partial private key for the sensor node. The partial private key is generated by using the identity ID of that node and a master key. KGC is also responsible for sending that partial private key to correct entity. They also described an adversary model to proof the security of their scheme. They used bilinear Diffie-Hellman problem as a base to the security of their scheme. Because their scheme was based on bilinear pairing, their scheme was not much efficient because pairing operation is much more costly that normal multiplication and exponential operation.

Xueying Zhang et al. [15] looked at the energy efficiency of different symmetric key cryptographic algorithms utilizing both stream cipher method and block cipher method in the case where security is being applied to the link layers of WSN's. They calculated the computational energy cost of stream and block ciphers by comparing the count of CPU cycles required to perform the encryption of given plaintext.

C. Karlof et al. [7] focused on secure routing, some attacks and their countermeasures in wireless sensor networks. They kept in mind two measure attacks like sinkhole attack, flood attack and analyzed secure routing protocols against these attacks. Other than these they described these attacks:

- Spoofed, altered or replayed routing information during communication in wireless sensor networks.
- Selective forwarding of information.
- Sybil attack
- Wormhole attack
- Blackhole attack
- Spoofing of acknowledge.

They also described crippling attacks against wireless sensor networks and suggested countermeasures and design considerations for them. They specified that most of proposed routing protocols of wireless sensor networks are venerable to intruder attacks. They kept open these problems to designers to create secure routing protocols. They stated that Link layer encryption techniques and authentication mechanisms could be the first approximation for providing security against mote-class outsider attacks, but only cryptography is not more than enough to provide all

security measures. There could be a possibility of laptop class and insider's attacks about them, designers should be careful.

He Debiao et al. [17] indicated that while using the bilinear pairing during generation of certificate-less signature schemes, the cost of pairing process is 20 times more than simple linear multiplication and exponential operations in RSA and elliptic curve cryptography techniques. They also stated that these schemes are more efficient and more practical that techniques using bilinear pairing for sign generations in certificate-less signature schemes. They also prove the security of their scheme using random oracle model using elliptic discrete logarithm problem.

Jinhong Zang et al. [5] proposed an efficient RSA based Certificate-less scheme on 2011 which used Strong RSA assumption and discrete logarithm problem to prove the security of scheme. Their scheme consists of 7 polynomial time algorithms. For the public and private key generation of the nodes, they used a secret value randomly selected by the node which is only known to that node only to remove the key escrow problem in ID based crypto-systems. According to Zang et al. their scheme was secure under Type I and Type II attacks but if we provide enough power to attacker, their scheme is not secure under type I attack. Other than this their scheme also has the problem of Signer's public key which was identified by Chin-Chen et al. [8].

To overcome the insecurity form Type I attack in [5], Gaurav Sharma et al. [9] presented a new certificate-less scheme. In this scheme they modified Zang scheme by modifying $R_1 = [(H_0(ID))^e]^{r_1}$ to $R_1 = x_{ID}^e[(H_0(ID))^e]^{r_1}$ and corresponding value of u_1. By doing this they were able to secure their scheme against Type I attack by this modification increased their signing phase computation cost. Sharma et al. also used strong RSA assumption in random oracle model to prove the security of their scheme against Type I and Type II attacks. Researchers provided different variations on developing and improving the performances of certificate-less signature scheme in [12, 14, 16, 17, and 18].

3. FUTURE SCOPE

A key challenge during the design of this was how to propose a scheme which can provide maximum security with less overhead and to minimize computational complexity.

So in this monograms we are taking one assumption that BS is working as KGC and verifier which is fixed and contains unlimited power source which is a possible scenario in case of WSNs. As we know that RSA based schemes are easy to implement as compared to pairing schemes, so we are modifying Zang et al. [5] RSA based scheme with less computation and making our proposed scheme secure against Type I attack also.

Emerging security issues in WSN such as authentication, energy efficient protocol, QoS, and Localization. Cryptographic based schemes can be applied in various important applications such as Grid computing, Cloud Computing, Blockchain etc.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "*Wireless sensor networks: A survey*," Computer Networks, vol. 38, pp. 393–422, Mar. 2002.

[2] S. Al-Riyami and K. Paterson, "*Certificateless public key cryptography*," in Advances in Cryptology (ASIACRYPT'03), Lecture Notes in Computer Science, vol. 2894, pp. 452–473, 2003.

[3] F. Amin, H. Jahangir, and H. Rasifard, "*Analysis of public-key cryptography for wireless sensor networks security*," vol. 2, no. 5, pp. 403–408, 2008.

[4] X. Chen, K. Makki, K. Yen, and N. Pissinou, "*Sensor network security: A survey*," IEEE Communications Surveys Tutorials, vol. 11, no. 2, pp. 52–73, 2009.

[5] J. Zhang and J. Mao, "*An efficient rsa-based certificateless signature scheme*," Journal of Systems and Software, vol. 85, no. 3, pp. 638–642, 2012.

[6] A. D. Wood and J. A. Stankovic. "*Denial of service in sensor networks*." IEEE Computer, 35(10):54–62, Oct. 2002.

[7] C. Karlof and D. Wagner. *"Secure routing in wireless sensor networks: Attacks and countermeasures.*" Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, 1(2–3):293–315, 2003.

[8] Chin-Chen Cheng, Chin-yu Sun and Shih Chang, "*A strong RSA-based and certificateless-based Signature scheme*", International Journal of Network Security, vol.0, no.0, pp. 1-7, 2014.

[9] G. Sharma and A. Verma, "*Breaking the rsa-based certificateless signature scheme*," Information-An International Interdisciplinary Journal, vol. 16, no. 11,pp. 7831–7836, 2013.

[10] Gaurav Sharma, Suman Bala, and Anil K. Verma, "*An Improved RSA-based Certificateless Signature Scheme for Wireless Sensor Networks*", International Journal of Network Security, vol.0, no.0, pp. 1-8, Apr 2014.

[11] J. Tsai, N. Lo, and T. Wu, "*Weaknesses and improvements of an efficient certificateless signature scheme without using bilinear pairings*," International Journal of Communication Systems, vol. 27, no. 7, pp.1083–090, July 2014.

[12] R. Tso, X. Huang, and W. Susilo, "*Strongly secure certificateless short signatures*," Journal of Systems and Software, vol. 85, no. 6, pp. 1409–1417, 2012.

[13] R. Tso, X. Yi, and X. Huang, "*Efficient and short certificateless signatures secure against realistic adversaries*," The Journal of Supercomputing, vol. 55,no. 2, pp. 173–191, 2011.

[14] J. Walters, Z. Liang, W. Shi, and V. Chaudhary, "*Security in Distributed, Grid, and Pervasive Computing,"* Chap. 17 Wireless Sensor Network security: A survey, pp. 1–51, CRC Press, 2007.

[15] X. Zhang, H. Heys, and L. Cheng, "*Energy efficiency of symmetric key cryptographic algorithms in wireless sensor networks*," in 25th Biennial Symposium on Communications (QBSC'10), pp. 168–172, 2010.

[16] Z. Zhang, D. Wong, J. Xu, and D. Feng, "*Certificateless public-key signature: Security model and efficient construction,*" in Applied Cryptography and Network Security, Lecture Notes in Computer Science, vol. 3989, pp. 293–308, 2006.

[17] D. He, J. Chen, and R. Zhang, "*An efficient and provably-secure certificateless signature scheme without bilinear pairings*," International Journal of Communication Systems, vol. 25, no. 11, pp. 1432–1442, 2012.

[18] D. He, M. Khan, and S. Wu, "*On the security of a rsa-based certificateless signature scheme*," International Journal of Network Security, vol. 15, no. 6, pp. 408–410, 2013.

[19] Yann glouche, Thomas Genet and Erwan Houssay, IRISA, "*SPAN A Security Protocol Animator for AVISPA,*" Sep 2008.

[20] C. Wang, D. Long, and Y. Tang, "*An efficient certificateless signature from pairings,*" International Journal of Network Security, vol. 8, no. 1, pp. 96–100,2009.

[21] P. Gong and P. Li, "*Further improvement of a certificateless signature scheme without pairing*," International Journal of Communication Systems, vol. 27, no. 10, pp. 2083–2091, Oct. 2014.

[22] Bellare, Mihir Rogaway, Phillip "*Random Oracles are Practical: A Paradigm for Designing Efficient Protocols*". ACM Conference on Computer and Communications Security:pp 62–73 1993.

[23] Y. W. Law, "*Key Management and Link-Layer Security of WSN*", Ph.D. Thesis, University of Twente, Netherland, 2005.

[24] K. Koyama and R. Terada, "*How to Strengthen DES–Like Cryptosystems against Differential Cryptanalysis*,"Transactions of the Institute of Electronics, Information, and Communication Engineers, v. E76–A, n. 1, Jan 1993, pp. 63–69.

[25] J.A. Gordon, "Strong Primes are Easy to Find," *Advances in Cryptology:* Proceedings of EUROCRYPT 84,Springer–Verlag, 1985, pp. 216–223.

[26] R.L. Rivest, A. Shamir, and L.M. Adleman, "*A Method for Obtaining Digital Signatures and Public–KeyCryptosystems,*" Communications of the ACM, v. 21, n. 2, Feb 1978, pp. 120–126.

[27] A. Fiat and A. Shamir, "*How to prove yourself: Practical solutions to identification and signature problems,"* in Advances in Cryptology—CRYPTO '86,vol. 263 of LNCS, pp. 186–194, Springer-Verlag, 1987.

[28] FIPS 180-2, "*Secure hash standard*." Federal Information Processing StandardPublication 180-2 (Draft), NIST, US department of commerce, 2001.

[29] FIPS 186, "*Digital signature standard*." Federal Information Processing Standard Publication 186, NIST, US department of commerce, 1994.

[30] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. Tygar,SPINS*: security protocols for sensor networks,* in: Proceedings of Mobile Networking and Computing 2001, 2001.

[31] L. Chen and J. Malone-Lee, "*Improved identitybased signcryption*," in Proceedings of Public KeyCryptography - PKC '05, vol. LNCS 3386, pp. 362 379, Springer-Verlag, 2005.

[32] M. Toorani and A. A. B. Shirazi, "*Cryptanalysis ofan elliptic curve-based signcryption scheme*," International Journal of Network Security, vol. 10, no. 1, pp. 51–56, 2010.

[33] Zhang, Z., Wong, D.,*"Certificateless public-key signature: security model andefficient construction.*" In: Zhou, J., Yung, M., Bao, F. (Eds.), ACNS 2006. LNCS, vol. 3989. Springer, Heidelberg, pp. 293–308, 2006.

[34] Yuan, Y., Li, D., Tian, L., Zhu, H.,"*Certificateless signature scheme withoutrandom oracles.*" In: ISA 2009, LNCS 5576, pp. 31–40, 2009.

[35] E. Edition, E. Edition, O. Systems, S. Edition, B. D. Communications, and S. Edition, THE WILLIAM STALLINGS BOOKS ON COMPUTER DATA AND COMPUTER COMMUNICATIONS , EIGHTH EDITION. .

[36] A. Cryptography and T. Ciphers, Foreword by Whitfield Diffie *Preface Chapter 1 — Foundations Part I — Cryptographic Protocols Chapter 2 — Protocol Building Blocks Chapter 3 — Basic Protocols Chapter 4 — Intermediate Protocols Chapter 5 — Advanced Protocols.*

[37] R. Mukesh, "*Blackhole Attack prevention using random dispersive routing for mobile adhoc networks,*" vol. 2, no. 4, pp. 77–87, 2012.

[38] A. Kumar, P. Sharma, S. Chatterjee, and J. Kanta, "*A dynamic password-based user authentication scheme for hierarchical wireless sensor networks*," J. Netw. Comput. Appl., vol. 35, no. 5, pp. 1646–1656, 2012.

[39] K. Xue, C. Ma, P. Hong, and R. Ding, "*A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks*," J. Netw. Comput. Appl., vol. 36, no. 1, pp. 316–323, 2013.

[40] K. Shim, Y. Lee, and C. Park, "*Ad Hoc Networks EIBAS : An efficient identity-based broadcast authentication scheme in wireless sensor networks*," Ad Hoc Networks, vol. 11, no. 1, pp. 182–189, 2013.

[41] Y. Gao, P. Zeng, and K. R. Choo, "*Multi-Sender Broadcast Authentication in Wireless Sensor Networks*," pp. 633–637, 2014.

[42] D. W. Carman, P. S. Krus, and B. J. Matt. "*Constraints and approaches for distributed sensor network security*". Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood, MD, 2000.

[43] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler. "*Spins: security protocols for sensor networks*". Wireless Networking, 8(5):521–534, 2002.