International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-1, November 2019

A Systemic view of One-Pass Cryptographic Key Distribution Techniques for WSNs

Manoj Ranjan Mishra, Amit Vijay Kore, Jayaprakash Kar

***Abstract:** The availability and use of cheaper and smaller sensors has brought an evolution in the field of Wireless Sensor Networks. The changes occurring in the environment can be observed, recorded through the large-scale deployment of sensor nodes that can build-up the much-required information system. Also, they are able to monitor and congregate data about the living organisms therein. In near future, millions more devices are expected to be connected. We focus upon the security services required by WSNs that are most challenging as compared to other networks. First, we introduce the commercially used motes with the comparison of technical and implementation related issues. Second, we analysed the variants of existing one-pass key management protocols for the resource constrained devices. Our aim is to provide a new direction to WSN Security through a restricted key distribution mechanism.*

***Keywords:** Forward Secrecy, Implicit Key Authentication, key distribution, Known/Unknown key Security, Motes, One-pass key Establishment, Wireless Sensor Networks*

I. INTRODUCTION

In the last few years, our planet has become more crowded and has gone through a lot of changes. The constituent parts of the earth i.e. land, oceans, atmosphere, polar regions and life are responsible for the planet's natural cycles and deep Earth processes [1], which now also includes human society. The rise in global temperature has led to melting of ice and increase in sea levels. The whole world is now facing extreme weather and water disasters. The basic requirements such as food, water and clean air are being affected by global change. The future may become far scarier than the simple rise in temperatures. Indeed, many such issues require solutions and strategies to effectively manage the planet's physical, chemical, biological and social components. It may become possible with the help of technological advancements that can quantify the changes occurring by sensing and processing the data.

The combined effort of both engineering and science, in the harsh climatological condition including the daily normal conditions, has provided us with the instruments that can be used to detect, acquire, control and analyse environmental conditions. The instruments/ sensors be able to withstand extreme environments and supply us with the most accurate information. Now a days, many such sensors are available that can measure the changes occurring in the physical environment like temperature, cold, pressure, vibration, humidity, sound etc. that can predict the climates and alert us about incoming natural disasters.

Technologies have evolved with a slope of steady scientific changes depending upon the market applications to fulfil the requirements of the society. The growth of wireless technologies with a strong base of theoretical framework have helped the evolution of sensor networks that can be applied for the automation and industrial usage. Currently, Wireless Sensor Networks (WSNs) are going through a more rugged phase driving its development and large-scale ubiquitous deployments. The availability of low-cost sensors has enabled voluminous deployment of WSNs in scientific and consumer applications that has also culminated the emerging Internet of Things (IoT).

The Sensors are classified based on their usage characteristics, material and technology like: Temperature, Flow, Proximity, Displacement, Image, Moisture, Force, Viscosity, Gas and Chemical etc. The MEMS, CMOS and LED sensors that are available, can thus be used to track and control the environmental conditions.

The widespread use of WSN technology, brings with its various vulnerabilities and possible threats from an adversary in a networked environment. Many such issues are investigated and described here while considering the advantages provided by the WSNs, to be used in a more efficient manner. First, we give an overview of the sensor networks and then discuss about the classical security protocols, attacks and their counter measures.

II. WSN OVERVIEW

Wireless Sensor Networks (WSNs) are defined as a self-configured and infrastructure-less wireless networks containing sensing, computing and communication elements that aim to give its controllers the ability to measure, collect and react to occurrences in the monitored environment. A sensor is a piece of equipment that can detect, the changes or happenings around or nearby, measure, record it and present them as a usable output. Usually, the sensor(s) are connected to a computing machine through a wire or wireless connection that stores the output from a sensor for further analytics and decision making. A team of researchers from the University of California at Berkeley in 1999 [2] combining the concept of micro-sensing with wireless communication, developed Rene (by CrossBow Technologies), named it as smart dust what we now refer to as Wireless Sensor Nodes or Motes [3].

Revised Manuscript Received on November 30, 2019.
* Correspondence Author

Manoj Ranjan Mishra*, School of Computer Applications, KIIT, Bhubaneswar, India. Email: mrmishrafca@kiit.ac.in

Amit Vijay kore, Research Scholar, School of Computer Engineering, KIIT, Bhubaneswar, India. Email: amit.kore88@gmail.com

Jayaprakash Kar, Department of Computer Science and Engineering, The LNMIIT, Jaipur, India. Email: jayaprakashkar@gmail.com

Further collaborative effort of industry and academics has resulted in building modern large-scale smart sensor networks, henceforth referred to as Wireless Sensor Networks (WSN) technologies. Examples of such initiatives include:

- UC Berkeley - PicoRadio program (1999)
- mAMPS - Project at MIT (2000)
- NASA - SensorWebs (2001)
- ZigBee - ZigBee Alliance (2002)
- CENS - Center for Embedded Network Sensing (2002)
- RFID - Radio-frequency identification (2005)
- 6LoWPAN - IPv6 over Low power Wireless Personal Area Network (2007)
- ANT - Short wireless communication (2012)
- BLE - Bluetooth lower energy (2012)
- DASH7 - v1.0 of the DASH7 Alliance Protocol (2015)
- Bluetooth Mesh Networking - allows for many-to-many communication over Bluetooth radio (2017)

A. WSN Applications

These initiatives along with the integration of Micro-Electro-Mechanical Systems Sensors (MEMS) and the availability of various physical, chemical and biological sensors have provided us with a large number of promising application areas [4]. A few modern sensing applications are categorized below:

- Military: Control and monitoring the friendly forces, battlefield observation, inspection of opposing forces, damage evaluation, Nuclear, biological and chemical (NBC) attack detection and targeting.
- Environmental: Monitoring oceanic, soil and atmospheric conditions, earth and planet exploration, detection of forest fire and pollution control.
- Health: Observation of a person’s bodily processes, tracking and monitoring and providing patients information to doctors in a hospital.
- Residential area Automation: manage household devices locally and remotely.
- Agriculture: Sensors and their networks can successfully increase the food production to satisfy the multiplied demand for food. The sensors are can be used to: Collect weather, crop and soil information, Monitoring of distributed land, Irrigation, Fertilization etc. [5]
- Commercial Applications: Monitoring product quality; environment control inside an office building; robotic control and guidance in manufacturing; industrial process control and instrumentation; coordination during disaster management; transportation and tracking the vehicles etc.

B. The Motes

A Mote consists of 8/16-bit processor with an EEPROM to act as non-volatile flash memory, external power source (battery), A/D converter (for sensor and actuator) and a radio transmitter [6], assembled into a package. They are made to be simple, non-obtrusive, embeddable in any environment and dynamically reprogrammable. The motes are able to connect and co-operate according to various models and architectures [7]. The key requirements of a mote are quite obvious, such as its ability to capture, process, store and forward the data automatically along paths integrated with the network infrastructure. A representative diagram is shown in Figure 1.

TinyOS is an embedded, component-based Operating System, a core component at the heart of a mote that supports various ambient intelligent systems by successfully addressing the challenges of WSNs. This OS provides interfaces among interconnected modules for common functions such as sensing, actuation, routing the packets and storage along with the ability to deploy a self-configuring network of devices.

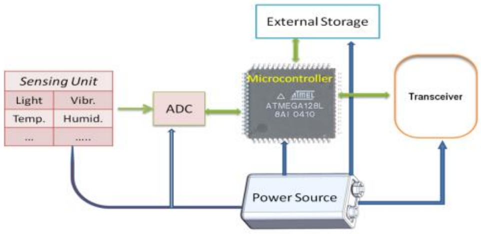

Figure 1: A Sensor Node

C. Sensor Nodes

A Mote and a Sensor collectively work as a Sensor Node and henceforth referred to as nodes [8]. The sensor nodes are made viable with the emerging miniature technology, wireless transmission and digitization of electronic components that consists of tiny, low-price, low-power devices [9]. The nodes are deployed within a range for communication depending upon the applications like habitat monitoring, smart home & consumer electronics, security, military surveillance, environmental sensing, hospitals etc. They offer smart control based on the supply of accurate, instantaneous measurements to lower the energy requirements. Hence, the extensive adoption of Wireless Sensor Networks (WSNs) will revolutionize the way people live [10].

D. Architecture of Sensor Networks

A Sensor Network consisting of small nodes can be deployed randomly in a remote environment or in a predetermined area of operation (land, underwater, underground) where the nodes do collaborate with each other to send data to the user [11]. These nodes are capable of sensing continuously, while communicating not only raw captured data but also partially validated and processed data with other nearby nodes via wireless medium. The unique and improved features of nodes endow us with many promising application areas, despite the constraints imposed by sensor networks. A typical WSN is shown in Figure 2.

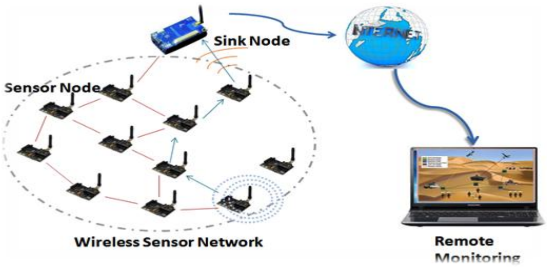

Figure 2: Typical Wireless Sensor Network Scenario

Realization of such networks need careful design of protocols that has engaged many researchers. Also, there are many other factors that influence the planning, implementation and deployment of a sensor network. The possibility of a nodes failure in a network can't be avoided but it should not affect the overall network operation. The requirement of the number of nodes for some applications may range up to an extreme value of millions, eventually imposes scalability issues. For large scale implementation the production cost of a node needs to be kept low, possibly less than US$1. Apart from its small size, the nodes must consume extremely low energy. The ease of deployment, its ability to operate unattended being adaptive to the extreme environments, are among other requirements [12, 13].

Topology: - For a realistic WSN application, individual nodes in the network must be reachable in order to perform its task efficiently. Alike ad-hoc networks, multi-hop routing strategies are adopted that addresses the communication issues. Indeed, after deployment the topology for connectivity and coverage are of utmost importance. The coverage topology, describes the coverage and a reliable sensing area of operation and is concerned about how to maximize it while consuming less energy. The connectivity topology emphasizes on the message retrieval and delivery mechanism in the network. The power control/management mechanisms are suggested to control the radio power level and to maintain a good wake/sleep schedule to realize optimized connectivity and reduced energy consumption [14]. A WSN mostly operates on battery power, hence it is very crucial to its usefulness in terms of availability and lifetime of the network. Network lifetime can be increased by efficiently controlling the energy consumed by each individual node of the network [15], since the existence of the node is dependent on the lifetime of the battery. Hence, topology control is posed as a major issue. Also, the response time in a secured sensor network is a critical issue. The alarm messages with high priority must be sent immediately at any cost despite the low power operation mechanism.

E. WSN Platforms

Whenever researchers have tried to achieve levels of security, apart from its cost, it suffers a lot in terms of processing overheads and adequate memory requirement to perform cryptographic computations as it involves operations on thousands of bits. But WSN nodes that are designed to perform under constrained resources, do require a lightweight or optimized mechanism that has higher levels of security and to consume less energy. In order to implement the cryptographic primitives, the processor should be able to perform arithmetic operations on large integers efficiently. So, selection of hardware among the various motes available is equally important.

Crossbow MICAz Mote module: (Now taken over by MEMSIC [16]): MICAz, is a 8-bit low processor platform that operates within the 2.4 GHz band and capable of being operated as a router. Also, it works as a base station with an interface to a standard PC. The MPR2400CA model equipped with the ATmega128L from Atmel, a low-power microcontroller can execute MoteWorks from its internal storage. The 51-pin slots, supports a wide selection of sensors and data acquisition and UART interfaces provides attachments for various external peripherals. The MICAz (MPR2400) equipped with IEEE 802.15.4 radio, is designed to offer both high speed transmission (up to 250 kbps) and security using AES-128 encryption.

MoteWorks™ allows the implementation of customizable sensor applications with the help of the TinyOS and provides for reliable, (ad-hoc) mesh networking, cross development tools and a user interface to analyse and to configure.

TmoteSky [17], is equipped with a 16-bit powerful processor and a wide variety of sensors attached to the main PCB that provides for increased performance, functionality expansion and TinyOS support. Its key Features are:

- 250kbps data rate, 2.4GHz
- IEEE 802.15.4 radio, an onboard antenna with 100m range
- 8MHz, MSP430 microcontroller with 10k RAM and 48k Flash.
- Integrated ADC, DAC, Supply Voltage Controller, DMA Controller
- Light, Humidity and Temperature sensors
- Consumes very low energy
- Faster wakeup from sleeping state (< 6ms)

Imote2 [18], is the most powerful (32-bit Processor) sensor platform that is more capable than the previously discussed nodes. It comes with the low power PXA271 XScale CPU and also attached to it with an IEEE 802.15.4 compliant radio and 2.4GHz Antenna.

Table 1: Features of Various Motes

Motes/ Features	MICAz	Tmote Sky/TelosB	Imote2	SHIMMER	IRIS
CPU	Atmega128L	MSP430	PXA271	T1 MSP430	Atmega1281
Processing	8 bit	16 bit	32 bit	16 bit	8 bit
Program memory	128KB	48KB	32MB	48KB	4KB
RAM	4KB	10KB	256KB	10KB	8KB
FLASH	512KB	1MB	32MB	none	512KB
MicroSD slot	None	none	none	2GB	-
Clock speed	8MHz	8.19MHz	13MHz	4-8MHz	8MHz
Radio	CC1000	CC2420	CC2420	CC2420	AT86RF230
Frequency (ISM Band)	2.4 GHz	2.4 GHz	2.4 GHz	2.4 GHz	2405 to 2480 MHz
Data rate	250kb/s	250kb/s	250kb/s	250kb/s	250kb/s
Current Draw (Processor)	8 mA	1.8mA (TelosB)	31mA	-	8mA
Weight W/O Battery (g)	18	23	12	10	18
Weight with Battery (g)	63.82	68.82	80.73	10.36	69.4
Battery Type	2x AA	2x AA	3x AAA	coin cell	2x AA
Price (Approx.)	US$99	EUR90.00	-	EUR199	US$115
Model	WSN-PRO2400CA	TPR2420CA	IPR 2400CA	-	XM2110CA

The most common features of various popular motes are presented in Table 1, but the actual specification of motes that are available today may vary from one model to other. These typical motes with 8 or 16-bit processors having only 4KB of data memory and 48KB of program memory, it is really very difficult to incorporate the security primitives except the only Imote2 that comes with high-end platform. Another important aspect we could not ignore, is the consumption of power during wireless transmission of encrypted data by the sender node as well as reception and decryption of ciphertext by the receiver node. Hence our aim is to find an ideal security solution for sensor nodes.

Although computationally powerful microcontrollers like PXA271 and ARM920T comes with word size of 32 bits, more than 256kB of RAM memory and 4MB of instruction memory that can accommodate the symmetric and asymmetric primitives but power consumption during awake is more than 44mA as compared to MSP430F16x and ATmega128L microcontrollers that consumes only 8mA.

F. Data Management in WSNs

The architecture of WSN [4], based upon the deployment strategy can be categorized as Data acquisition network and the Data Dissemination Network. First one is supposed to collect data from the environment and transmit them with minimal or no recessing to the base station. The other one may be connected to wired or wireless network that provides an interface to the data acquisition network. Various deployment strategies [19] for the WSNs are:

- *Collect and Transmit* (Simple model) - The nodes sense the data and the values are simply sent, directly to the base station with minimal data processing.
- *Collect and Forward model* - Each node is supposed to collect the data values that are followed to the base station, being routed through the intermediate nodes.
- *Self-Organizing model* - During the last decade many new devices have come up like sensors that triggers the development of new applications with increasing communication complexities, to fulfil our day-to-day needs. For a unmanned environment, it sometimes requires the nodes ability to organize itself as per the network topology or randomly and can perform node discovery, routing and maintenance.
- *Data fusion model* - provides for an energy optimization technique by reducing communication to the aggregating nodes where a group of nodes forming one cluster, collects environmental data that are aggregated at the cluster heads and then sends the only packet to the central collection point.

G. Security Issues of WSNs

Wireless Sensor Networks can be deployed in wide variety of areas and most of these applications require physical security (tamperproof devices) and a secured data transmission and protection scheme for stored data [20]. In order to protect from stealing the data or leaking the sensor readings, packets can be encrypted using symmetric key mechanism and then can be sent from one node to other. The use of a key and hence key distribution is a crucial factor in building a secured channel for WSNs. Apart from hiding data during transmission, the node has to secure the internally stored data that may contain the secret key in its memory. Data integrity, i.e. protection from modification, needs to be achieved through authentication of entities and authentication of the key that ensures the actual identity of other parties so that the receiver is able to verify the sender. This requires both secure protection of the key and exact identification of those entities, having the right to use it [21].

Apart from these basic services, the WSNs are supposed to collect highly sensitive information from open or hostile environments that are vulnerable to attacks on the software and hardware, should be equipped with higher levels of defence mechanisms. As per the requirement of the applications, the sensor nodes are distributed being connected to each other via wireless links and collect data in a collaborative manner. These data packets are periodically transferred to a sink node, that works as gateways for further processing. In such a scenario, the possibility of active and passive attacks like injection of fake data or eavesdropping are quite obvious [22, 23]. Therefore, a great deal of research activities is being carried out to secure the WSNs with efficient mechanisms.

The tiny nodes are most often deployed in unattended hostile/toxic areas where they do interact with the environment to collect data and broadcast them through other nodes to the end-user. If large number of nodes are deployed, sometimes it becomes impossible to visit them after deployment. Hence, they are required to be configured carefully before deployment. The possibility of accidental failure of nodes or causing physical damage to the node can’t be avoided. Also packets when sent through wireless medium may suffer from interference and distortion, or dropping of packets due to congestion and a Denial-of-Service (DoS) attack from an adversary may affect the entire network, making it much difficult to fulfil its purpose.

Thus, collection of accurate and secured data through sensor nodes from harsh environment is a real challenge. A malicious adversary or an insider can manipulate the nodes or the channel because of the public as well as the distributed nature of the network. Any intentionally planted device can observe the flow of data and then try to tamper the nodes, modify and then retransmit packets, change the routes of packets and steal the identity etc.

H. Possible Attacks on WSNs

An attacker in WSNs may passively look for sensitive information by applying traffic analysis and monitoring, eavesdropping without affecting the natural flow of data in the sensor networks, thus remains beyond the knowledge of the user. But there exist various active attacks like DoS, flooding, alteration of data, fabrication, black hole, repeated transmission of packets, sinkhole, spoofing, jamming, overwhelm, man-in-the-middle attack, selective forwarding and fake node. Indeed, the attacker is able to take control over and can supervise all the communications from nodes [23, 24]. A few of them that are highly susceptible to side channel attacks are listed below:[25]

- Denial of Service (DoS): The adversary may try to disrupt the normal operation of the node or the entire network by sending superfluous packets and services become unavailable to the authorized users.
- Jamming: A kind of DoS attack whereby the jammer inserts RF signal with an intention of blocking the wireless channel, eventually preventing the sensitive or high priority information from reaching its destination.
- Blackhole/Sinkhole Attack: An attacker can get the access to stream of packets by implanting a powerful node to pull or misdirect all the packets, while listening and responding to routing requests from the deployed nodes and acting as a shortest path to BS while influencing the routing.

- Hello Flood Attack: A node belonging to the adversary with very high transmission range, sends HELLO packets to all reachable nodes. The victim nodes may confuse the attackers' node as a neighbour and use it during data transmission to BS.
- Wormhole Attack: is a threat to distance-based routing mechanism without compromising a node in the sensor network whereby the attackers' node attempts to provide a single-hop fake shorter route that can actually be reached through multihop. Hence it creates an illusion of a tunnel, where the two end points seem to be nearer than the actual distance.
- Node Subversion: If an adversary physically captures the node, then the possibility of revealing useful data along with the key stored in it cannot be avoided thus affecting the entire network.
- Node Malfunction and Outage: Any technical error in the node may produce erroneous data e.g. if the cluster head that is responsible for aggregation of data is malfunctioning or stops operating due to some or other reason, that poses as a threat to the integrity of WSNs.
- Sybil Attack: In Sybil attack [26] an adversary node with a malicious intention can illegitimately take on multiple identities that are either stolen from destroyed nodes or fabricated arbitrarily and acts as a different node that can be initiated during voting, distributed storage and data aggregation.
- Cut-and-Paste Attack: In the absence of hashing or proper authentication mechanism, an attacker can modify by altering the bits of an encrypted message and then sends it to the receiving node where the modified message gets decrypted without realizing the forgery.
- Oracle Attack: an adversary trickery applied upon a honest principal who inadvertently reveals some information. Hence, the honest principal is used as a tool by the adversary to gain information which otherwise she cannot possibly have obtained.

Another kind of attack by the insiders that should not be overlooked where the authenticated nodes can be misused for alteration, eavesdropping, misrouting or dropped packets etc. Hence security is essential to ensure the presence and reliable functioning of the nodes.

Routing data packets in WSNs are unreliable, since the link quality in wireless medium differ and the nodes may fail. If the nodes are deployed in large scale, it may require multiple hops to finally reach the destination (sink) node, eventually increases the power consumption and decreases the life time of the nodes. The packets:

- during transmission may get affected or lost due to channel errors.
- may clash during simultaneous broadcast from two or more neighbouring nodes.
- may suffer from latency due to multi-hop routing or network congestion.

So, scalability that influences the routing protocols need to be adaptive to the changes and must be designed to support the increased workload while keeping the nodes alive for a longer lifetime. There are many additional security attributes that are required for the security of any key establishment protocol. The specific key requirements are as follows:

- Implicit Key Authentication, the assumption whereby one party is sure that no other party aside from a precisely identified second party (and possibly additional identified trusted entity) may gain access to a particular secret key.
- Known (Session) Key Security. We also generally expect the adversary will be able to obtain session keys from any session other than the one under attack.
- Unknown Key Share Security. Infrequently the adversary may be unable to obtain any useful information about a session key, but can deceive the protocol principals about the identity of the peer entity.
- Forward Secrecy. When the long-term key of an entity is compromised the adversary will be able to masquerade as that entity in any future protocol runs. However, the worst situation may arise if the adversary can also use the compromised long-term key to obtain session keys that were accepted before the compromise. Protocols that prevent this are said to provide forward secrecy.
- Key Compromise Impersonation Resistance. Another possibility may rise if the long-term key of an entity A is compromised i.e. the adversary may be able to masquerade not only as A but also to A as another party B. Such a protocol is said to allow key compromise impersonation.

WSNs have put many new challenges because of its major design obstacles. The study of these challenging issues provides for the base to work on secured sensor networks. The individual sensors with very limited resource available in it are required to execute complex algorithms or programs. For example, the MCS410CA, is a locality aware module of MICAZ low-energy Processor/Radio Cricket mote [27] has an 8-bit Atmel ATMega128L processor operating at a speed of 8 MHz with 4KB of RAM, 128KB of Program memory and 512KB of FLASH storage. For such type of resource constrained device, the size of the software must also be small, fast and energy efficient.

III. EXISTING CRYPTOGRAPHIC MECHANISMS

The security of data in a network involves, the encryption/ decryption of data using symmetric key schemes like 3DES, AES, where the two nodes within a range for communication need to share a 'secret key' and has diverse requirements like processing capability, time, word length, memory, key length, etc. and hence, its suitability of use for a sensor network is essential. As seen in, [28] only a few algorithms can be fit into these nodes. Some block ciphering algorithms run on a fixed-size block of bits while others operate as stream of individual bits or a byte at a time and goes through various rounds of continual operations with their subkeys.

Any two entities with their associated identities that wishes to establish a secured communication link needs a shared key which is used till the end of a session. For multiple sessions or communication with other parties, a fresh (unique) key is required that involves interaction among them using key establishment protocols.

A. Key Establishment Protocols

For conventional networks, there are three categories of popular key sharing techniques: trusted third-party, self-enforcing and redistributions of keys. A trusted third-party mechanism depends on a trusted entity (server) for key conformity among the communicating entities. But these traditional key distribution and key exchange protocols with the help of trusted third-parties is not a good idea for large-scale sensor networks that is based on infrastructures. In the absence of a stable infrastructure, securing and managing the independent nodes of a sensor network bring with it a great challenge. Although, one major advantage here is that the actual user of the network is available as a trusted third party for key distribution that can pre-install a single mission-key for all. But if the nodes are managed remotely, the likelihood of physical attack (e.g. Physical tampering) is more than a traditional PC and impossible to detect. Indeed, symmetric key solutions fail when a few nodes are physically captured by attackers. The self-enforcing protocols, relies on public key techniques like Diffie-Hellman key exchange [29] or certification using RSA [30] that requires enormous computation, memory and energy from tiny sensor nodes. The third one is key pre-distribution, where distribution of keys occurs prior to deployment of nodes and seems to be feasible for WSNs. A wider view is given below.

For a secure communication between two adjacent nodes the most conventional protocols use pair-wise shared secret keys in the context of symmetric encryption by adopting a key pre-distribution mechanism [31]. First of all, a mesh network requires pre-distribution and a minimum storage space for nearly (n-1) keys in an individual node and $n(n$-$1)/2$ per WSN, that blocks the storage space and sounds impractical for large-scale WSNs. Secondly, it is hard to decide the sensor nodes that will be neighbours in specific applications. Hence pre-distribution of a very large number of shared secret keys for all neighbourhood pairs is not a feasible solution. In another way, each node may be installed with a master secret key prior to deployment that can be used to acquire a new pairwise secret key. Such a scheme could not protect the nodes from node capture attacks and the attacker may eventually disrupt the entire network through the captured node. Some researchers suggest hardware level alternatives for storing the master keys but
they are not safe always.

A downside of the symmetric key mechanism is the need for a secured key exchange algorithm to achieve its goal in WSNs. A preferred technique in asymmetric cryptosystem, referred to as Public Key Cryptography (PKC) comes to the rescue that generates two different keys: (a known Public Key and a secret Private key) being tied to a key ring. The generation of such a pair of keys can be accomplished through RSA [30] and ElGamal [32].

RSA, the most widely used algorithm, is observed to be computationally expensive for the tiny nodes and a minimum of 2048 bits key size is mandatory. ElGamal encryption, based on the complexity of calculating discrete logarithms, can be used but the key size is also equivalent to RSA scheme. As presented by Gura et. al. [33], Elliptic Curve Cryptography (ECC) using pseudo-Mersenne primes fields (a curve defined by the equation $y^2 = x^3+ax+b$), provides for smaller key lengths, faster addition/multiplication, along with lower memory requirement, energy consumption and bandwidth savings. ECC has provided us with primitives like ECDSA for signature and ECDH for key agreement. The major advantage of ECC scheme is the scalar point multiplication that can be accomplished through point addition and doubling. The length of the resulting message to be transmitted using ECC's 160-bit key was found to be shorter than RSA's 1024-bit key. Indeed, well-matched for smaller devices.

A feasible solution to this is to enforce the continuation of a public key infrastructure (PKI) in WSNs. In traditional PKI the certification authorities (CA) are responsible for authentication of public keys through a signed certificate that carries the identity and the public key of the specific node. But the deployment of PKI in WSNs is not easy due to its networked nature (decentralized) and requires various functional units like Certification & Registration Authority (CA/RA), a Certificate repository and a certificate management system.

Munivel & Ajit [34] proposed a micro PKI, a lightweight implementation of PKI for WSN whereby the base station (BS) is required to be authenticated exclusively with the use of a pair of keys [35]. The sensors in the network use the public one (key) to authenticate the BS, while the BS uses its own private key to decrypt the data sent by sensors which ensure its confidentiality. It is claimed to be energy saving and ensures significant threshold of security. In order to set up secure tunnels between sensors, the researchers have proposed sensor to sensor handshakes that is managed and controlled by the base station. The BS being responsible for Registration, Certification, digital signature for certificates and other management activities like validation of certificates to check whether they have been revoked, it would be a costly affair for the BS for these PKI related communications.

B. Random key pre-distribution

Key pre-distribution is a mechanism where the keys are decided a priori from an initial keying material (e.g. any type of unique information or an algorithm that generates keys) or from a key-pool (list of keys). In static keying mechanism the keys once assigned by the manufacturer or by the base station are not updated after initial deployment. In dynamic key establishment scheme the keys are established by a fixed pair (or group) of entities on demand that also varies during subsequent runs and is also referred to as session key establishment.

Eschenauer and Gligor [31] has proposed a revolutionary efficient probabilistic distribution scheme, "random key pre-distribution," whereby each node is supplied with a random subset of keys and their IDs from a larger set of keys (pool) prior to deployment. Any two nodes can exclusively select a common key from within their subsets using the key discovery mechanism and use it as their shared secret key for communication after deployment and one of the remaining keys from the key ring can be used as a path-key. If a greater number of keys are compromised then a greater number of links also get affected. The support for re-keying was also suggested with the help of a key revocation mechanism for the compromised or expired keys.

Other researchers have proposed new means of key distribution schemes addressing the storage issues like the q-composite random key pre-distribution scheme, multi-path key reinforcement scheme and random pair-wise key scheme [36] to enable node-to-node authentication. The first one, assumes that any two nodes in its subset, have at least q number of keys and one of them can be chosen to set up a secure link. The link can be confirmed by matching their respective node IDs for authentication and pre-distribution requires at least q shared keys between a pair of nodes for establishing a secured link. The second one uses multiple indirect routes to set up a secure link. This method increases the number of communication links eventually increasing the energy consumption and overburdens the level of security in the network. These shared keys after its distribution, can't be used always (conventionally, session keys have a limited lifetime) and also needs to change the expired keys with re-keying those nodes that enforces another overhead on the sensor networks [37].

In [38], a deterministic scheme for a larger network is suggested that relies on key matrix manipulation and named it as symmetric key generation system (SKGS). Each entity is supplied with a low volume of secret information from which a pair of nodes can obtain its pairwise key that uses only (λ +1) memory spaces where, $\lambda < n$. The other nodes in the network are secure until the adversary compromises at least l nodes e.g. if more than λ nodes are compromised, the entire network gets affected. Hence the resilience against the node capture depends on the value of λ.

An Energy-Efficient dynamic Key Management (EEDKM) scheme [39], based on Exclusion-Based System (EBS) and t-degree bivariate polynomials, provides for rekeying locally (within a cluster) and can be performed infrequently. This does not affect or propagate to the other clusters of WSN. Since it uses a secret key between the BS and cluster heads (sensor node), it can authenticate the nodes and executes rekeying without consuming more energy. EEDKM still has computational and communication overheads.

A Location-Aware Combinatorial key management (LACKM) scheme [40] relies on Exclusion Based System (EBS) whereby the cluster heads (gateways) performs key refreshing for the nodes under its control, through the exchange of few messages only. A powerful command node authenticates the cluster heads that are fixed at a known location ensures communication reliability. It also enables a trade-off between the number of keys stored and the volume of network traffic due to the rekeying operations. The potential of collusion has been reduced by grouping the nodes based on their geographical location, eventually eliminates the requirement to store a large number of keys at every node.

A Hierarchy-based dynamic key management scheme (HDKMC) [41] is based on Hierarchical cluster architecture and Splay tree-based rekeying mechanism. This scheme performs better by saving more energy through dynamic management of keys at runtime phase by observing the current status of the node. It can also reduce the frequent exchange of messages for key renewals but requires special very powerful (high-energy) nodes.

A Key management scheme with the help of the deployment knowledge (KMDK) [42] for WSNs, suggests formation of hexagonal grids consisting of equal group of nodes and can make use of stored secret information of neighbour nodes more efficiently to supply pairwise keys. KMDK can achieve a better connectivity with a short-range communication and a lower memory requirement and is resilient against node capture. However, getting prior deployment knowledge for many applications is intricate.

In a Traffic-Aware Key establishment Scheme for WSNs [43] can setup shared keys for the active sensor nodes only that actually has data to be transmitted because most of the nodes might be sleeping after unnecessarily acquiring a shared key where the key is rarely used. Hence it wakes up only those necessary nodes, based on the topology information of the network but requires use of RTS/CTS frames to control the network.

IV. ONE-PASS KEY ESTABLISHMENT

In two-pass or multi-pass authenticated key establishment mechanisms, both the parties have to perform at least one round of communication in order to establish a session key [44, 45].

In One-Pass key establishment, the sender computes a session key SK and an associated message. The computed values are required to be transmitted to the specific entity using the its public key and sender's secret key. From the received components the receiver computes the SK again, that is the same as the one computed by the sender, using sender's public key and the other party's secret key.

Data that are gathered within the sensor network, are very precious and sensitive. Hence, in order to safeguard these collected data or messages that are transmitted between any two neighbouring nodes, an efficient and secured cryptographic protocol that supports mutual authentication and key establishment is essential. The existing protocols attempts to establish a Pairwise key/ Two-Pass Key between any two nodes that wishes to communicate. The energy consumed during the wireless transmission of a byte of data from a sender is comparable to executing 3000 CPU instructions by a general processor. One-Pass Key is a new paradigm where the Key Establishment can be implemented while communicating in one direction only, where the sender and the receiver compute the same key at their own end. i.e. the receiver calculates the key from some secret values, received from the sender.

Many key exchange algorithms e.g. DH protocol that either suffers from Man-in-the-middle attack or lacks authentication. If we use signature schemes and public key infrastructure for achieving authentication then it becomes computationally heavy as well as complex for the resource constrained devices in WSNs. We have incorporated a new means to key control using Identity-Based cryptography mechanism in this thesis, contributing to the construction of an efficient one-pass key establishment protocol and its security validation.

In order to apply security services and to implement the security mechanisms in WSNs is a great challenging job. Although, the traditional cryptographic techniques have provided us with many solutions like symmetric-key, public-key, key distribution and authentication techniques, still key distribution requires new solutions during transmission of data from one node to another.

The efficient use of keys during encryption and decryption, depends completely upon the secure and efficient key distribution mechanisms in WSNs. Hence our endeavour, in securing the key distribution process through the proposal of a new protocol, will be able to safeguard the nodes from various kinds of possible threats and attacks.

The network protocols for WSNs needs to be designed carefully for efficient and effective use of nodes. Given an application and the coverage area, assessment of the number of nodes to be used and the range between the nodes e.g. the decision of a topology becomes very important. In an ideal situation, the number of motes that varies from a few to several hundred, are usually deployed much closer to each other to reduce the energy requirement to transmit the packets. Since battery is the main power source of the nodes, the lifespan for many applications depends upon the algorithm's computational complexity, frequency of operation and communication overhead.

A. Existing One-Pass Key Establishment Protocols

The very need for security in the modern wireless devices (nodes), designing a secure and efficient One-pass key agreement protocol has been a challenging job. Amongst the numerous attempts made by researchers, the best-known methods to one-pass key establishment protocols include:

- KEA: The Key Exchange Algorithm (KEA) designed by the NSA. [46]
- Unified Model: The one-pass variant AK protocol. [47]
- MQV: proposed an efficient protocol for authenticated key agreement. [48]
- HMQV: a variant of MQV protocol. [49]
- OPAK: The protocol claims to achieve the highest level of security with one-pass mechanism against a wide variety of security attacks, at the expense of slightly higher computational cost. [50]
- KE-WR: Two protocols are proposed: a novel suite of One-Pass Key Establishment Protocol.[51]
- Gorantla: an ID-based key exchange protocol that allows a set of parties to agree upon a secret session key over a public network.[53]

A comparative study of the security aspects and the vulnerabilities of existing One-pass key establishment mechanisms have been discussed here and the summary is presented in Table 2.

Table 2: Assessment of variants of One-pass methods

*Scheme	IKA	PFS	KKS	UKS	KcI	LoI
KEA	✓	x	✓	x	x	x
Unified Model	✓	x	✓	✓	x	x
MQV	✓	x	✓	x	x	x
HMQV	✓	x	✓	x	x	x
KE-WR-I	✓	P	✓	x	P	x
KE-WR-II	✓	✓	✓	x	✓	x
Gorantla	✓	✓	✓	x	✓	x
OPAK	✓	x	✓	x	x	x
Mishra [52]	✓	✓	✓	✓	✓	✓

**IKA*: Implicit Key Authentication, *PFS*: Perfect forward secrecy, *KKS*: Known Key Secrecy, *UKS*: Unknown Key Share, *KcI*: Key-compromise Impersonation, *LoI*: Loss of Information, *P*: Partially Satisfied

We have gone through a few key establishment protocols that uses Diffie-Hellman and Identity-based schemes where, authentication primarily relies on long-term keys that can be correlated with identities like passwords or biometric information. Three different architectures have been generalized. The nodes may already have a shared secret key that is used during encryption or message authentication (MAC) or an off-line server be used to pre-distribute public key certificates that binds the key to the node's identity or a trusted server can share the key whenever data transmission is required. Hence the key must be in possessions of the two parties intending to communicate, in addition to the trusted server but no other adversary. Also, the protocol must assure the two (possibly unidentified) nodes have acquired the same key (session key).

V. CONCLUSION

In this paper, we provide the taxonomies of key management schemes for WSNs, along with their issues. We have emphasized upon the key distribution schemes and observed the existence of only a few One-Pass key establishment protocols for WSNs and some of them are found to be only the variants of these protocols. Therefore, a gap in this area of research inspired us to inscribe and motivated us to carry forward our work towards the development of secured key establishment protocols for low processor devices.

REFERENCES

1. Knight, J. R., Allan, R. J., Folland, C. K., Vellinga, M., & Mann, M. E., "A signature of persistent natural thermohaline circulation cycles in observed climate," Geophysical Research Letters, Vol.32, no.20, 2005.
2. Kahn RHKJM and KSJ Pister, "Mobile networking for smart dust," In ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 99), Seattle, 1999.
3. V Veena Madhuri, Syed Umar, and P Veeraveni, "A study on smart dust (mote) technology," In International Journal of Science, Engineering and Computer Technology, Vol.3, no.3, pp.124, 2013.
4. Chien-Chung Shen, Chavalit Srisathapornphat, and Chaiporn Jaikaeo, "Sensor information networking architecture and applications," IEEE Personal communications, Vol.8, no.4, pp. 52-59, 2001.
5. Abu Zafar Abbasi, Noman Islam, Zubair Ahmed Shaikh, et al., "A review of wireless sensors and networks' applications in agriculture," Computer Standards & Interfaces, Vol.36, no.2, pp. 263-270, 2014.
6. S Gowrishankar, TG Basavaraju, DH Manjaiah, and Subir Kumar Sarkar, "Issues in wireless sensor networks," In Proceedings of the World Congress on Engineering, Vol.1, pp. 978-988, 2008.
7. Luis Ruiz-Garcia, Loredana Lunadei, Pilar Barreiro, and Ignacio Robla, "A review of wireless sensor technologies and applications in agriculture and food industry: state of the art and current trends", In sensors, Vol.9, no.6, pp. 4728-4750, 2009.
8. Martin Turon, "Mote-view: A sensor network monitoring and management tool," In the Second IEEE Workshop on Embedded Networked Sensors, 2005, EmNetS-II., pp. 11-17, 2005.
9. Ian F Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, "Wireless sensor networks: a survey," In Computer networks, vol.38, no.4, pp. 393–422, 2002.
10. Franck L Lewis, "Wireless sensor networks, Smart environments: technologies, protocols, and applications," pp. 11-46, 2004.
11. Matthias Ringwald and Kay Romer, "Deployment of sensor networks: Problems and passive inspection," In Intelligent Solutions in Embedded Systems, 2007 Fifth Workshop on, pp. 179-192. IEEE, 2007.
12. Joseph M Kahn, Randy H Katz, and Kristofer SJ Pister, "Next century challenges: mobile networking for smart dust," In Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking, pp. 271-278, ACM, 1999.

13. Marcos Augusto M Vieira, Claudionor N Coelho, DC da Silva, and Jos´e Monteiro da Mata, “Survey on wireless sensor network devices,” In Emerging Technologies and Factory Automation,” In Proceedings. ETFA’03. IEEE Conference, vol.1, pp. 537-544. IEEE, 2003.
14. Maxim A Batalin and Gaurav S Sukhatme, “Coverage, exploration and deployment by a mobile robot and communication network,” In Telecommunication Systems, vol.26, no. (2-4), pp. 181-196, 2004.
15. Roger Wattenhofer, Li Li, Paramvir Bahl and Y-M Wang, “Distributed topology control for power efficient operation in multihop wireless ad hoc networks,” In INFOCOM 2001. Twentieth annual joint conference of the IEEE computer and communications societies. Proceedings. IEEE, vol.3, pp. 1388-1397, IEEE, 2001.
16. *Micaz datasheet*, MEMSIC, http://www.memsic.com/userfiles/files/Datasheets/WSN/micaz_datasheet-t.pdf, (accessed March 7, 2018).
17. *Tmote Sky Datasheet*, https://insense.cs.st-andrews.ac.uk/files/2013/04/tmote-sky-datasheet.pdf, (accessed March 7, 2019).
18. *Imote2*, Datasheet, (accessed March 7, 2019) http://wsn.cse.wustl.edu/images/e/e3/Imote2_Datasheet.pdf,
19. DC Jinwala, Dhiren R Patel, and KS Das Gupta, “A survey of the security issues in wireless sensor networks,” ADIT Journal of Engineering, Vol.3, no.1, pp. 17-29, 2006.
20. K. CHELLI, “Security issues in wireless sensor networks: Attacks and countermeasures,” In Proceedings of The World Congress on Engineering, vol.1, 2015.
21. Alfred J Menezes, Tatsuaki Okamoto and Scott A Vanstone, “Reducing elliptic curve logarithms to logarithms in a finite field,” IEEE Transactions on Information Theory, Vol.39, no.5, pp. 1639-1646, 1993.
22. Al-Sakib Khan Pathan, Hyung-Woo Lee, and Choong Seon Hong, “Security in wireless sensor networks: issues and challenges,” In 8th International Conference Advanced Communication Technology, vol.2, pp. 1043-1048. IEEE, 2006.
23. Ahmad Salehi Shahraki, MA Razzaque, Parisa Naraei and Ali Farrokhtala, “Security in wireless sensor networks: issues and challenges,” In Space Science and Communication (IconSpace), 2013 IEEE International Conference on, pp. 356-360, IEEE, 2013.
24. J.P. Walters, Z. Liang, W. Shi, and V. Chaudhary, “Wireless sensor network security: A survey, Security in distributed, grid, mobile, and pervasive computing,” Vol.1, pp. 367, 2007.
25. Mohamed-Lamine Messai, “Classification of attacks in wireless sensor networks,” arXiv:1406.4516, 2014.
26. K Abirami and B Santhi, “Sybil attack in wireless sensor network,” IJET, ISSN, pp. 0975-4024, 2013.
27. *Cricket mote Datasheet*, http://www.memsic.com/userfiles/files/Datasheets/WSN/6020-0082-02_a_cricket_kit-t.pdf, (accessed January 7, 2019).
28. J.P. Kaps, G. Gaubatz, and B. Sunar, “Cryptography on a speck of dust,” IEEE Computer, Vol.40, no.2, pp. 38-44, 2007.
29. Whitfield Diffie and Martin Hellman, “New directions in cryptography,” IEEE transactions on Information Theory, Vol. 22, no.6, pp. 644-654, 1976.
30. Ronald L Rivest, Adi Shamir, and Leonard Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Communications of the ACM, Vol. 21, no.2, pp.120-126, 1978.
31. L. Eschenauer and V.D. Gligor, “A key-management scheme for distributed sensor networks,” In Proceedings of the 9th ACM conference on Computer and communications security, pp. 41-47, ACM, 2002.
32. Taher ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” In Workshop on the Theory and Application of Cryptographic Techniques, pp. 10-18, Springer, 1984.
33. Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle, and Sheueling Chang Shantz, “Comparing elliptic curve cryptography and RSA on 8-bit CPUs,” In International Workshop on Cryptographic Hardware and Embedded Systems, pp. 119-132. Springer, 2004.
34. E Munivel and GM Ajit, “Efficient public key infrastructure implementation in wireless sensor networks,” In International Conference on Wireless Communication and Sensor Computing, ICWCSC-2010, pp.1-6, IEEE, 2010.
35. Benamar Kadri, Mohammed Feham and Abdallah Mahamed, “Lightweight pki for wsn mpki,” The Journal of Security and Communication Networks, Vol.10, no. 2, pp. 135-141, 2010.
36. Haowen Chan, Adrian Perrig, and Dawn Song, “Random key predistribution schemes for sensor networks,” In Security and Privacy, 2003. Proceedings. 2003 Symposium on, pp. 197-213, IEEE, 2003.
37. A Selva Reegan and E Baburaj, “Key management schemes in wireless sensor networks: a survey,” In Circuits, Power and Computing Technologies (ICCPCT), International Conference on, pp. 813-820, IEEE, 2013.
38. R. Blom, “An optimal class of symmetric key generation systems,” In Workshop on the Theory and Application of of Cryptographic Techniques, pp. 335-338, Springer,1984.
39. Jong-Myoung Kim, Joon-Sic Cho, Sung-Min Jung, and Tai-Myoung Chung, “An energy-efficient dynamic key management in wireless sensor networks,” In The 9th International Conference on Advanced Communication Technology, vol.3, pp. 2148-2153, IEEE, 2007.
40. M.F. Younis, K. Ghumman, and M. Eltoweissy, “Location-aware combinatorial key management scheme for clustered sensor networks,” IEEE transactions on Parallel and Distributed Systems, Vol.17, no.8, pp. 865–882, 2006.
41. Yiying Zhang, Xiangzhen Li, Jianming Liu, Jucheng Yang, and Baojiang Cui, “A secure hierarchical key management scheme in wireless sensor network,” International Journal of Distributed Sensor Networks, SAGE, 2012.
42. Zhen Yu and Yong Guan, “A key management scheme using deployment knowledge for wireless sensor networks,” IEEE Transactions on Parallel and Distributed Systems, Vol.19, no.10, pp. 1411-1425, 2008.
43. Dijiang Huang, Manish Mehta, Deep Medhi, and Lein Harn, “Locationaware key management scheme for wireless sensor networks,” In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, pp. 29-42, ACM, 2004.
44. Mishra, M.R., Kar, J. and Majhi, B., “Practical deployment of one-pass key establishment protocol on wireless sensor networks,” International Journal of Pure and Applied Mathematics, Vol.100, no.4, pp.531-542, 2015.
45. Michel Abdalla, Jens-Matthias Bohli, Maria Isabel Gonzalez Vasco and Rainer Steinwandt, “(password) authenticated key establishment: from 2-party to group,” In Theory of Cryptography Conference, pp.499-514, Springer, 2007.
46. NIST Skipjack, “KEA algorithm specifications,” 1998.
47. Richard Ankney, Don Johnson, and M Matyas, “The unified model, Contribution to X9F1,” 1995.
48. Laurie Law, Alfred Menezes, Minghua Qu, Jerry Solinas and Scott Vanstone, “An efficient protocol for authenticated key agreement, Designs, Codes and Cryptography,” Vol.28, no.2, pp. 119-134, 2003.
49. Hugo Krawczyk, “HMQV: A high-performance secure diffie-hellman protocol,” In Annual International Cryptology Conference, pp. 546–566, Springer, 2005.
50. Konstantinos Chalkias, Spyros T Halkidis, Dimitrios Hristu-Varsakelis, George Stephanides and Anastasios Alexiadis, “A provably secure onepass two-party key establishment protocol,” In International Conference on Information Security and Cryptology, pp. 108-122, Springer, 2008.
51. Yuan Wang, Duncan S Wong, and Liusheng Huang, “One-pass key establishment model and protocols for wireless roaming with user anonymity,” International Journal of Network Security, Vol.16, no.2, pp.129-142, 2014.
52. Mishra, M.R., Kar, J. and Majhi, B., “Practical deployment of One-Pass key establishment protocol on wireless sensor networks”. International Journal of Pure and Applied Mathematics, Vol 100, No.4, pp.531-542, 2015.
53. M Choudary Gorantla, Colin Boyd, and Juan Manuel Gonz´alez Nieto, “Id-based one-pass authenticated key establishment,” In Proceedings of the sixth Australasian conference on Information security, Vol.81, pp.39-46. Australian Computer Society, 2008.

AUTHORS PROFILE

Manoj Ranjan Mishra, http://orcid.org/0000-0003-2282-5778 He has completed his M. Tech. in Computer Science from Utkal University, India. and Ph. D. from KIIT Deemed to be University, India in Computer Science. Currently he is working as Associate Professor at School of Computer Applications, KIIT Deemed to be University, Bhubaneswar, India. His research interests are on design and development of cryptographic protocols for low processor devices, IoT, Network and Cloud security.

Amit Vijay kore, Received his Bachelor’s degree from KIT’s Collage of Engineering, Kolhapur and master’s degree in Engineering from the University of Pune, India. He is currently perusing his research work in the School of Computer Engineering, KIIT, Deemed to be University, Bhubaneswar, India. and working as Assistant Professor at AISSMS Collage of Engineering, PUNE, India. Network management, Security and energy harvesting in WSNs are among his research interests.

Jayaprakash Kar, http://orcid.org/0000-0003-4800-4791 Completed M. Sc. and M. Phil. in Mathematics from Sambalpur University, M. Tech. and Ph. D. in Computer Science (Cryptographic Protocols) from Utkal University, India. Currently he is working as Associate Professor in the Department of Computer Science and Engineering, The LNM Institute of Information Technology, Jaipur, India His current research interests is on development and design of provably secure cryptographic protocols and primitives using Elliptic Curve and Pairing based Cryptography includes digital signature, Signcryption Scheme, Key management problem of broadcast encryption, Deniable authentication protocols, Proxy Blind Signature scheme.