A Survey on Security Architecture and Key Management Systems in a Wireless Sensor Network

Sunil Kumar[†] , C. Rama Krishna[††] and A. K. Solanki[†††],

Research Scholar, I. K. Gujral Punjab Technical University, Kapurthala (Punjab), INDIA
Department of Computer Science and Engineering, NITTTR, Chandigarh, INDIA
Department of Computer Science and Engineering, BIET, Jhansi (U.P.), INDIA

Summary
With the enhancement of digital communication, Wireless Sensor Networks (WSNs) use various security techniques to offer infrastructure secure data transmission. Conversion of data files into different format using cryptography, hash function and pattern generation techniques are the common practices to facilitate high data security. Mostly, such transformations as well as retrieval of original information rely on symmetric or asymmetric key pairs. Together with the advancement of security approaches, distinct successful or unsuccessful efforts have been made by numerous illicit third parties to assess the transmitted data and secret keys unethically, disturb the transmission process or distort the transmitted data and keys. Seldom, the limitations of communication channel, transmitting and receiving devices play an important role to dilute data security. Hence, in this paper we review the existing data security architecture and key management system in WSN. Based on this review and current security gaps, this paper suggests a probable integrated solution for secure transmission of data and secret keys to address these limitations.

Key words:
Cryptography, hash function, pattern generation, symmetric/asymmetric key, data security architecture, key management system.

1. Introduction

Wireless sensor is an evolving technology that can be applied where manual efforts cannot be apprehensive such as monitoring of traffic, fire retort, armed forces command and others serious applications. A distinct number of topologies that are used in networks such as mesh, tree, star etc. are also used in WSN communication systems to make data transfer rate faster. Apart from that, data security is another major aspect in any communication system. In WSN, implementation of required security mechanism is not an easy task due to its resource restricted nature. However, encryption, virtual private network (VPN), firewalls, diverse authentication mechanisms are the popular security approaches to protect data from the external threats as a first line of defense during communication in WSN (Jokhio et al. (2013)[1], Bashir et al. (2013)[2], and Rezvani et al. (2015)[3]).

An Intrusion Detection System (IDS) is a vibrant system for monitoring that is used to inspect, recognize and perceive illegal actions such as notching transmitted data, efforts to break the security barrier during transmission, creations of disturbances during transmission and so on (Mahmood et al. (2014)[4], Seo et al. (2015)[5] and Dutta et al. (2014)[6]). It ascertains breach and prohibited access, address distinct issues related to data confidentiality, integrity, authentication, approval, unavailability and allocation of resources. In wireless sensor networks, the existing literature shows that there is a trade-off between efficient resource consumption and improved security mechanism of sensor networks. On the other hand, if the network security is increased during the communication, then we have to agree on competent resource feasting or vice versa (Tong et al. (2010)[7], Amokrane et al. (2011)[8] and Yin et al. (2015)[9]).

Depending upon the nature of diverse threats in WSN communication, the existing security techniques are categorized into two types, such as inside security and outside security. Inside security means safe transmission between the sensors and base stations. In this scenario, base stations are treated as reliable destinations. Outside security means safe transmission of data or message between the WSN base stations and the outside users such as subscribers of WSN services. The key characteristics of outside security are integrity and availability of data (Tong et al. (2010)[7], Amokrane et al. (2011)[8] and Yang et al. (2010)[10]).

According to Jokhio et al. (2013)[1], Amin et al. (2016)[11] and Ismail et al. (2013)[12], security during data transportation in WSN can be further categorized into layered approach, i.e., distinct security frameworks and encryption based security techniques. Special securities are needed in tiny sensor nodes with the use of different approaches of developing security framework such as hash function, pattern generation technique and distinct error control mechanisms. In layer based approach, the three used layers are Physical Layer (or Radio Stack Layer), Data Link Layer or MAC Layer (which deals with issues such as scheduling of time control of power and

Manuscript received April 5, 2017
Manuscript revised April 20, 2017

synchronization along with nodes) and the Application Layer (which is quite precise to the WSN usage and deployment environment) (Rezvani et al. (2015)[3], Assaf et al. (2016)[58] and Mu et al. (2016)[54]).

Liu et al. (2013)[13], Udgata et al. (2011)[14] and Liu et al. (2012)[15], have discussed in their articles about the different security layers of WSN, various key management techniques accessible and their applicability in sensor networks. The primary limitations regarding authenticity, scalability and confidentiality which stop the conventional key organization and distribution techniques to apply in sensor network can be reckoned as restricted processing and memory, scalability and unique communication patterns. The general practices to manage the key in WSN are master key, preconfigured symmetric keys; network wide shared key, link key management, bootstrapping keys and public key cryptography. In network wide shared key, every node uses a single network wide symmetric key. Consequently, in link keys and master key scheme, every network node is reconstructed by using a master key. Public Key Cryptography is a traditional key management scheme where the use of Diffie-Hellman key exchange technique is very popular. In preconfigured symmetric key management system, every network node is preconfigured with a set of link keys with which it will setup a protected links with other nodes. Bootstrapping keys allows on demand key creation for a protected link recognized between the nodes (Ahmed et al. (2011)[16], Saleem et al. (2011)[17] and Seo et al. (2015)[5]).

However, there are many limitations in various key management and security schemes, used in WSN communication systems. Henceforth, this paper reviews the strengths and limitations of current security techniques and distinct key management schemes. The particular objectives for this paper are:

- To analyze the strength of distinct current security techniques and key management systems, used in WSN communication.
- To point out and addressing the current limitations of exiting security and key management systems.
- To propose a probable integrated solution to address these current limitations.

Rest of the paper is structured as follows. Section-II contains the background study to analyze the strengths and weakness of different security techniques and key management systems, Section-III proposes a probable security integrated solution to address the current limitations of distinct security techniques and key management schemes. Section-IV concludes the paper with directions to future work.

2. Background Study

It can be seen that the data security in WSN depends on the physical security of data and key management system. Henceforth, the security aspect of the WSN has been discussed in this paper according to the different security aspects and key management schemes. In this section, we have designed the following taxonomy, as shown in Fig.1, to present the structure of this study. The entire literature has been structured in this section according to the designed taxonomy to make it more precise and show the inter-relativity between the different security aspects of WSN.

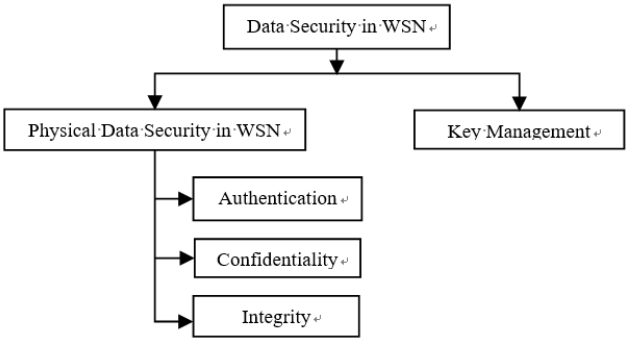

Fig. 1: Taxonomy for WSN security structure

In Fig.1, basic aspects of physical security, i.e., authentication, confidentiality and integrity are included. The discussion on physical data security of WSN is presented in section 2.1 and in the subsequent sub section 2.2 key management issues is included. Section 2.3 analyses the strengths and limitations of recently used techniques for data security in WSN environment.

2.1 Physical Data Security of WSNs

Data security in WSN (Yin et al. (2015)[9], Hoteit et al. (2015)[49] and Torii et al. (2016)[56]) relates to the prevention of data from unintentional or intentional changes, destruction or disclosure through the use of physical security, administrative controls, unauthorized controls, etc. So it becomes an important part for an organization or individual to manage the implementation and ensure its effectiveness. From the last several decades, different security techniques have been invented by different researchers. According to Yao et al. (2010)[21], Zheng et al. (2012)[22] and Branch et al. (2013)[23], these security techniques can be categorized depending upon the types of media (i.e., text, audio, video and image) and on the basis of security principles (i.e., authentication, authorization, confidentiality, integrity, non-repudiation and availability).

Data authentication is the activity of ensuring the originality for a single piece of data after receiving it at the receiving end. Actually it is the process of establishing the identity of data to prove the ownership (Karaman et al. (2012)[24] and Guizani et al. (2012)[25]). Here a unique identifier is sent to the receiving end with the segment of data to be authenticated. These identities may be encrypted by public key; in this case public keys are also sent with the encrypted identities. Authentication does not determine that what tasks the individual computer can do or what files the individual client computer expects. Different types of data authentication techniques so far have been used for different media authentication. Therefore data authentication techniques can be classified into four categories depending upon the different media, i.e., image, video, audio and text (Lai et al. (2015)[44], Ruikai et al. (2015)[48] and Freeda et al. (2016) [59]).

Among common authentication techniques based on PIN and password (Saleem et al. (2011)[17] and Zhuang et al. (2015)[46]), SMS based authentication using cryptography (Ding et al. (2010)[26] and Dwivedi et al. (2011)[27]), biometric authentication (Aivaloglou et al. (2009)[39] and Hoteit et al. (2015)[49]), use of message authentication code (Cai et al. (2011)[28]), use of digital signature (Miyaji et al. (2011)[29] and Amin et al (2016) [11]), use of hash function (Seo et al. (2015)[5] and Fakhrey et al. (2016)[51]) are most significant. Generally, these techniques are used for both weak and strong authentication systems. According to Lim et al. (2010)[30], Han et al. (2014)[31] and Kumar et al. (2016)[50], the strong authentication system involves two or more factors such as identification of senders, authenticity of received data and others. According to Ferng et al. (2014)[32] and Liao et al. (2010)[33], few network authentication protocols such as challenge handshake authentication protocol (CHAP), CRAM-MD5 (authentication methods supported by Simple Authentication and Security Layer (SASL)), Extensible Authentication Protocol (EAP), Kerberos, Host Identity Protocol (HIP), Password Authentication Protocol (PAP) and others are used for data authentication too (Mai et al. (2015) [47] and Li et al. (2016)[52]).

Consequently, confidentiality prevents the information to be revealed to the unauthentic user while it is transmitted to the actual user (Branch et al. (2013)[23], Das et al. (2012)[34] and Hou et al. (2016)[53]). Confidentiality means restricting sender's information between the sender and receiver and not to leak information to the other user. Some approaches such as distinct cryptography, Steganography, pattern generation and matching techniques, hash functions and other security techniques have been applied by the different researchers to increase confidentiality, (Marwaha et al. (2010)[35] and Berger et al. (2016)[55]). The two major approaches that are used to achieve confidentiality are Steganography and Encryption.

Primary part of information security is data integrity. In wide use, data integrity means correctness and consistency of the stored data in a database (Rangan et al. (2010)[36], Qazanfari et al. (2014)[37] and Jiaying et al. (2016)[57]).Data reliability can be described as a process, a status or a function which is used quite regularly as an alternative for data excellence. In this technique, data values are reconciled according to the respective data type or data model. Integrity of data is encroached within a database at the time of formation and valid through the continuous process of validation routines and error inspection. Data integrity is the process of verification that the data remain unchanged in transmission from sender to destination. According to the situation, data reliability is a measure of the substantiality and the commitment of a data item. As we know data integrity is directly related to the data error, which may be caused during the transmission time by the channel noise, extra overhead on transmission channels or may be environmental causes. Data error may also occur due to hardware cause. Data error can be of two types, i.e., single bit or multi-bit error. To solve this single or multiple bits error, several techniques are implemented by the different researcher's such as Parity Checking and Hamming Code (error correction mechanism). The multi bits error can be corrected using automatic repeat request (ARQ), repeated coding, cryptographic hash function, cyclic redundancy code etc.

The error control mechanism is further divided into two categories, i.e., detection and correction of errors. According to Tong et al. (2010)[7]. Udgata et al. (2011)[14] and Kalra et al. (2015)[45], in data transmission system, error detection is the procedure of identification of data errors; it may be single or multi bit, introduced into data by the channel noise or other impairments while transmission from source to destination. The error can be discrete or continuous among the data stream. There are several error detection techniques that are used to detect such types of errors such as parity checking, two-dimensional parity checking, checksum, cyclic redundancy check (CRC), longitudinal redundancy check (LRC),Hamming code (used for both detection and correction), use of cryptographic hash function (According to Ahmed et al. (2011)[16], Saleem et al. (2011)[17] and Freed et al. (2016)[59]). Error correction is the process of cleaning data file from errors which may incorporate during the transmission or storage. A number of techniques have been applied to prevent these errors such as forward error correction (FEC) and automatic repeat request (ARQ). Among which ARQ is simplest backward error rectification code. In this method, whenever the receiver receives the erroneous packets, the receiver sends the appeal of retransmission to the sender until all the

received packets become error free. The ARQ can be of three types such as Go-Back-N, Stop-and-Wait and Selective Repeat. Stop-and-wait ARQ is also called Alternating-Bit-Protocol and mostly used in telecommunication to transmit data between two connected devices. Go-Back-N sends acknowledgement of highest received in-order and corrected packet in more efficient way than stop-and-wait protocol. Selective Repeat acknowledges individual packet, however, it cannot control the corrupted packet.

With the rapid use of internet, transmissions of such electronic media files require to be compressed (lossy or lossless) for avoiding the transmission overhead and reducing channel congestion (Yang et al. (2010)[10], Liu et al. (2013)[13] and Lai et al. (2015) [44]). The data loss may occur due to it, and data integrity may suffer. Such compression techniques are very sensitive with respect to the transmission error. Sometimes corruption of one bit during the transmission may cause whole compress code uncompressible.

On the other hand, to enhance confidentiality, cryptography is widely used. Cryptography mainly depends on keys. Cryptographic keys are required to be managed by using a robust technique that guarantees the security requirements. So, initially all the necessary key required are distributed to the nodes before they are disseminated in the target area and then the sensors that need to communicate establish its secure communication by having a deal on what is called pair-wise key, and allow the refreshment process for those keys to be occurred successfully when it is needed, and finally, having the ability to revoke the keys that related to compromised nodes (Rezvani et al. (2015)[3] and Mu et al. (2015)[54]). These phases are collectively called key management. In this paper we will explain different key management schemes, critique them notionally, and propose an idea as a way out for the expected problems in one of these schemes.

2.2 Key Management

An important issue in WSN structure is the key management. WSN relies on the strength of the communicating devices, battery power and sensor nodes which have the ability to communicate in wireless environment over a limited region. Due to energy and memory limitations, construction of a fully functional network needs to be well arranged. A number of techniques are available in the current literature for such key management techniques. Among them distribution of key over the network, sharing of private and public keys are the most important (Ahmed et al. (2011)[16], Momani et al. (2010)[38] and Torii et al. (2016)[56]). These schemes focus on many phases that are needed to build a secure WSN environment and to overcome the aforementioned obstacles in it. A detail discussion of such schemes has been presented in the following sub section.

2.3 Analysis of current security schemes used for WSN

A sensor network is a big network of resource constrained sensor nodes with several stipulated tasks, such as processing and sensing. The current threats and solutions proposed to handle these threats are further discussed in this section to analyze their strengths and weaknesses. This section also helps to find the current research gap by analyzing the distinct drawbacks of such techniques and it also helps to build a technique for overcoming these limitations.

Sensor networks need well-built security infrastructure, as it is typically used in a serious, unfriendly and complex situation where humanoid effort cannot be applied (Khanum et al. (2012)[18] and Ruikai et al. (2015) [48]). Due to source and computing constraint, security in WSN needs attention. Henceforth, for the sensor network, authors proposed a detection system called Mobile Agent Based Hierarchical Intrusion Detection System (MABHIDS). By applying the least potential network capitals, intrusion detection of dual levels is accomplished in the projected technique. The proposed method enhances network lifespan by reducing the workload on cluster head as well as it also delivers enhanced level of security in sensor networks. However this technique is not robust against the external threats such as various active or passive security attacks such as Monitor and Eavesdropping, Traffic Analysis, Sybil Attacks and so on; distinct single or multiple bits transmission errors and others limitations of data transmission system in WSN environment (Seo et al. (2015)[5] and Torii et al. (2016)[56]).

Sensor synthesis offers correctness and robustness as well as it also generate distinct problems such as high costs and consume extraordinary amount of power and high execution time (Viani et al. (2010)[19], Mai et al. (2015)[47] and Amin et al. (2016)[11]). Hence, in order to shrink the hardware complexity to detect and track human activities to interact with active devices worn by the targets, the authors proposed WSN-based solutions for security and surveillance. This work focuses on WSN-based resolution for sensing of transceiver-free targets, which deals with the information offered by the wireless links among the nodes only. This technique offers higher accuracy and robustness against various transmission errors and offers great reliability against the various security threats. However, the proposed technique offers higher computational complexity which makes this

technique unsuitable where faster processing is required during the communication.

Depending upon clustering in WSN architecture, Zhenghong et al. (2010)[20] proposed a protected routing protocol with detection of intrusion, in which a power extrapolation model for sensor nodes is applied to identify attacks. It is used in the phase of cluster head selection and key management method to the point of cluster creation to guarantee nodes security. Whereas, for nodes, a flow forecast model is used to protect against traffic linked attacks in routing stage. The projected protocol can sense and protect against some elegant routing attacks such as Selective Forwarding, Wormhole, Sybil and Hello-flood attacks. In this technique, for cluster creation stage, key management is used and for nodes, a flow prediction model is used, which is further applied to defend against traffic attacks in routing phase. However, this technique is not efficient for controlling channel congestion. Above all, it cannot protect data loss which occurs due to channel noise, software and hardware limitations.

Inadequate region, low memory and low power of sensor networks put firm restraints on selecting cryptographic practices (Ahmed et al. (2011)[16] and Kalra et al. (2015) [45]). So, Elliptic Curve Cryptography (ECC) is preferred due to its small key size. High security in spite of compact key size results in power and area effectual crypto systems. In this work, for sensor networks, author demonstrates the hardware execution of Elliptic Curve based asymmetric cryptosystem. Field used for elliptic curve is defined over prime numbers. In this work, the CPU is designed keeping in view the evolving security necessities of WSN. This work is efficient to reduce the computational complexities; however, this technique is not efficient to protect against security attacks such as DDoS attacks, sniffer attacks.

In multi-hop sensor network, nodes or users regularly enter and leave the network (Saleem et al. (2011)[17] and Kumar et al. (2016)[50]). Traditional methods for controlling network management are not perceived to competently look such kind of threats. Henceforth as per author, innovative appliances are needed to build it in a self-structured style. The skills are initiated for environment potentials sensor network to self-adjust conservational deviations and self-protect from spiteful matters. This research introduces a biological inspired secure autonomous routing protocol (BIOSARP). In this particular research, the authors have also proposed a self-boosted routing protocol with Artificial Immune System (AIS) based safety mechanism. This approach improves sensor network in protecting itself from anomalies and common attacks in WSN during routing such as forwarding route requests, sending forged or modified route requests to the entire WSN and others. However, it is not perfectly capable of protecting against attacks like Sybil attack, altered attack, spoofing attack and replayed routing information attack.

A probability theory based trust model was proposed by Momani et al. (2010)[38]. The trust model based on Bayesian theory paid more interest due to simple inference. To deduce overall trust, Bayesian fusion algorithm is introduced to combine both data and communication trust. In the network, data trust value is based on the performance of sensor nodes. Data trust is called the distribution function value of the Gaussian distribution and communication trust is the trust value based on cooperation in routing messages between two nodes and this value is defined as the value (expected) of the beta reputation system (BRS). The BRS value is based on the beta probability density function. This system is proposed to enhance the trust level using the probability theory; however, it is not a realistic application to defend external security threats such as spoofing attack and sniffer attack.

Hybrid Trust and Reputation Management for Sensor Networks (HRMSN) overcomes the rigidity of a single identity based trust model and massive power consumption of a single behavior based reputation model (Aivaloglou et al. (2009)[39], Zhuang et al. (2015)[46] and Hou et al. (2016)[53]). In this model, when a node i need to set up a trust link with a new node j, then node i will investigate for a convincing certification center x to verify the new node j. If the certification is accepted, the node i will gather trust evidences of the node j. However, this technique involves high computational complexities.

TinyKey is developed to overcome the limitations of TinySec protocol (Corin et al. (2011)[40]). TinyKey is the first protocol in which the performance results are conducted on full-scale deployment. This protocol avails a key management method within the structural design of the protocol. This protocol uses KMS (Key Management Sub-module) for validating and saving new keys on the nonvolatile memory. For the validation of key, the version number of the message is compared with the version umber of the recent keys. The recent key will be replaced only if the version number of the new key is higher. CBC-MAC provides message integrity and authentication. Random key generator and Skipjack algorithm which provides message confidentiality and protection against reply attacks. It also supports Initialization Vector (IV) which prevents repetition in data encryption. However, this technique is unable to protect data loss due to extra data overhead and channel congestion as well as channel noise.

Use of a particular topology comprise distinct situations such as node breakdown and topology modifications to rejoin the broken nodes (Yin et al. (2015)[9]). Thus, topology fault tolerant state transfer model can be

established. Here authors proposed a new error tolerance assessment index of topology under different states depending upon the nature of topology giving network services. In this work primarily depending upon the semi-Markov process, the topology fault tolerant state transfer model is introduced due to response behavior and failure behavior of a topology. After that an innovative quantifiable error tolerance estimation index with calculated service characteristics of distinct topological states is projected. At last, the key issue affecting the error tolerance of topology is acquired applying the planned appraisal index. However on the designation of fault tolerant, this work was unable to calculate the topological service ratio. Hence, the acceptability of it to protect various transmission errors is uncertain.

The possibility of configurable software based on link layer security structure wherein an application can be compiled flexibly, with respect to its actual security demand is needed (Jinwala et al. (2009)[41], Hoteit et al. (2015) [49] and Fakhrey et al. (2016)[51]). Hence, authors proposed the fundamental design of such configurable link layer security structural design for sensor networks. Different aspects related to the proposed method viz. configurable MAC sizes, configurable block ciphers, configurable block cipher modes of operations and configurable replay protection are tested and verified in this scheme. The proposed architecture is intended to offer the most favorable level of protection at the minimum overhead, thus saving the valuable resources in the sensor networks. The overall contribution of this research work is in augmenting the link layer security framework for the WSN with the new concept of configurability. However, this work is not suitable in the security mechanism of sound files. The limitations in the post-deployment implementation impose the extra overhead during the communication process.

Sensor networks can interrelate with conscious data and drive in adverse unattended surroundings besides that it is authoritative that security matter be considered from the staring of the system (Sahana et al. (2011)[42], Li et al. (2016)[52]). As per authors, WSN also suffers with resource restraints because of their lack of energy and storage of data; however, both signify key problems to build the modern computer safety techniques in a sensor network. Hence there should be some negotiation between the energy and the safety. Hence, asymmetric key cryptographic algorithm RSA has been applied for sensor in an efficient method by using adjusted calculation. Nevertheless, in this proposed technique, the execution process requires considerably long time though it is efficient to offer higher security. The requirement of higher execution time makes it unusable for complex and large data sets.

According to Cui et al. (2014)[43] and Berger et al. (2016)[55], selective forwarding attacks influence the integrity of data transmission not by advancing a subset of received packets periodically. The discerning property changes selective forwarding attacks difficult to be categorized from the usual packet drops or improvised reception in an unstable situation of wireless. Hence, authors proposed suppress selective forwarding attacks in WSN. This technique is a sensitive routing mechanism that circumvents doubtful nodes by approximating maternal node's dependability and link excellence in a combined way. Here a set of logical prototypes has been established for ensuring the degree of which one can distinguish selective forwarding attacks from apparent packet drops due to instabilities of wireless channel. In this work, Node Reliability Estimator (NRE) has been construed and scrutinized for classifying spiteful and apprehensive selective forwarding nodes, and further assimilated it with link excellence approximation to suggest a metric for new routing. An algorithm for sensor node rank has also been established to regulate the greatest perilous sensor node positions, when negotiated the network agonizes the maximum influence of selective forwarding attack. This work studies the intuitions on how various selective forwarding nodes can disturb sensor network functions even in case of multi-sink networks. Nevertheless, the proposed scheme has high time complexity which is impractical for a real time system. Apart from that it increases high data overhead for what packet loss may occur, which is also unlikely (Jiaying et al. (2016)[57], Yingxu et al. (2015)[44] and Assaf et al. (2016)[58]).

Secure service and management for security-critical WSN is an integrated approach and constructed depending upon the security facility as well as the management for enhancing the data security in security-critical WSN (Liu et al. (2012)[15]). As the consequence, this work offers security solution which can be employed against distinct attacks, used in WSN environment. This technique facilitates several features such as shares keys over the network, combines keys along with the information and comprises feather weight public key pre-distribution scheme, hop by hop packet signature and encryption in the route path, distant management of nodes besides data confidence and network path analysis. However, this technique cannot protect against attacks like spoofing and DDoS (Distributed Denial-of-Service) attack. Moreover this technique is not feasible for tiny devices, where the amount of storage space is low (Rezvani et al. (2015) [3]) and Kumar et al. (2016) [50]).

Security model for sensor networks using zero knowledge protocol is used to address few distinct security attacks and threats in sensor networks such as replay and man-in-the middle attack (Udgata et al. (2011)[14] and Seo et al. (2015)[5]). It is a technique for finding the distributed

sensor cloning attack and utilization of zero knowledge protocol for validating the validity of sensor nodes of the sender. In this technique, addressing of cloning attack is done by affixing a distinctive finger print to every node depending on the set of adjacent nodes and itself. The zero knowledge protocol is used to make sure non communication of critical cryptographic data in the wireless sensor network to avoid replay and man-in-the middle attack. Nonetheless, this technique is not capable to protect against distinct passive attack such as traffic analysis attack, non-evasive eavesdropping and monitoring of transmissions. On the other hand, this technique is also not applicable for real time system where TinyOS and Tossim are used.

Henceforth, from the above discussion of this section, we have seen that these exiting techniques have distinct limitations in terms of time and space complexities, implementation costs and energy consumptions during the execution (Mai et al. (2015)[47] and Torii et al. (2016)[56]). Though these techniques are purposefully used to solve certain security issues, however they cannot solve the issues related to data integrity, data confidentiality and information loss in an integrated way. Even in few occasions, employment of certain security techniques can create another security issues, for example, use of complex encryption technique enhances data confidentiality, but reduces data integrity by incrementing the data loss. Similarly, highly efficient data compression technique reduces data size efficiently, but it liquefies the data confidentiality. Therefore, considering all these additional factors and existing literature gaps, this research work suggests a probable integrated solution to address various security issues related to information loss, data confidentiality and data integrity in the following section.

Table 1: Comparison of Security Architecture and Key Management

Authors	Pros & Cons
Mai et al. (2015) & Torii et al. (2016)	distinct limitations in terms of time and space complexities, implementation costs and energy consumptions during the execution
Udgata et al. (2011) & Seo et al. (2015)	sensor networks using zero knowledge protocol is used to address few distinct security attacks and threats in sensor networks such as replay and man-in-the middle attack
Liu et al. (2012)	an integrated approach and constructed depending upon the security facility as well as the management for enhancing the data security in security-critical WSN
Jiaying et al. (2016) , Yingxu et al. (2015) & Assaf et al. (2016)	High time complexity which is impractical for a real time system. Apart from that it increases high data overhead for what packet loss may occur, which is also unlikely
Cui et al. (2014) & Berger et al. (2016)	Selective forwarding attacks influence the integrity of data transmission not by advancing a subset of received packets periodically.
Sahana et al. (2011) and Li et al. (2016)	Interrelate with conscious data and drive in adverse unattended surroundings besides that it is authoritative that security matter be considered from the staring of the system
Jinwala et al. (2009), Hoteit et al. (2015) & Fakhrey et al. (2016)	Configurable software based on link layer security structure wherein an application can be compiled flexibly, with respect to its actual security demand is needed
Yin et al. (2015)	particular topology comprise distinct situations such as node breakdown and topology modifications to rejoin the broken nodes
Corin et al. (2011)	TinyKey is developed to overcome the limitations of TinySec protocol
Aivaloglou et al. (2009) , Zhuang et al. (2015) & Hou et al. (2016)	Rigidity of a single identity based trust model and massive power consumption of a single behavior based reputation model
Momani et al. (2010)	To deduce overall trust, Bayesian fusion algorithm is introduced to combine both data and communication trust.

3. Probable Integrated Solution

From the literature study of Section II, we have seen that a number of security techniques and key management schemes have been applied for secure data transfer in WSN environment. However, the existing limitations in these schemes transfigure them unusable. Henceforth to address the current issues belonging to the existing security techniques for WSN environment, this research work suggests a probable integrated security solution. In this probable solution, first of all we generate a symmetric

key for encrypting the input data. In the next stage the input file is encrypted using elliptic curve cryptography technique. The authenticity and the security level of the communication are then tested with the Diffie-Hellman key exchange technique. This part of the proposed technique also passes the secret keys from the sender to the receiving end. Finally, after establishing the secure connection between the sender and the receiver, the secret cryptic text is transferred to the receiving end. Fig. 2 shows the detailed steps about the probable integrated solution.

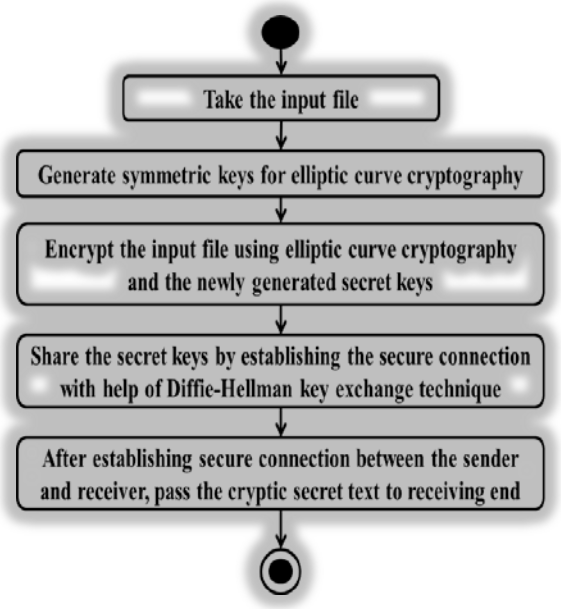

Fig. 2 Proposed integrated model to enhance the security level in WSN environment

In the next step of this research, we will implement our proposed integrated technique in WSN environment and test the performances of it in diverse aspects. The application of this proposed technique will enhance the data security by authenticating the user as well as the source before establishing any secure connections. Consequently, the technique can protect data during the transportation over network by protecting various security attacks against the data confidentiality such as packet capturing, port scanning and ping sweeps, phishing and others as well as it can enhance the robustness against the data loss by protecting various transmission errors. Apart from that the current security techniques are too complex in terms of time and space to apply them for securing data transmission between the tiny devices, used in WSN. These techniques are involving too much iteration during the executions which enhance the data as well as time over head considerably. However, the low life battery devices cannot afford such enhanced security overhead. Henceforth, the proposed security technique offers a fruitful solution to secure data transmission among the low battery life and tiny devices, used in WSN due to its low time and space complexities. This technique can be used in various security applications in wire sensor network environment such as financial transaction, research and development, and other governmental activities where high level of security is needed.

4. Concluding Remarks

This paper reviews current techniques related to existing physical security systems and key management mechanisms for WSN. According to the strengths and weaknesses, this research analyzes recent security techniques, used in WSN to avoid diverse manmade or machine made security hazards. Consequently, this research analyzes and explores the merits and demerits of recent security techniques. This analysis helps to point out the current research gaps in the field of data security and key management issues of WSN environments. With the basis of analyzing the strengths and weaknesses of current security techniques and current research gaps in the field of WSN data security, this research proposes a probable integrated solution for offering and managing the private or public keys in the Wireless Sensor Network. This probable solution also helps to address the distinct limitations of current security techniques and helps to control various transmission errors, information loss. The probable solution also includes a secure key management scheme to enhance data security and safety.

The proposed technique can be applied for establishing the secure connection in wireless environment where high level of security is needed such as financial transaction, banking system. As the proposed technique is applicable for the tiny and heavy devices, hence, it is suitable for mobile banking. The proposed scheme is also useful for scientific research where high level of security is needed to transfer input sample or experimental results.

Further extension of this research work is to implement the proposed integrated technique in various WSN architectures. The performances of the proposed integrated technique in different aspects will be tested after implementing it and will be tested for the suitability of it in both small and substantial devices. The power consumption during entire execution is the key factor which makes this research suitable in WSN environment. Henceforth, power saving capacity will be tested and compared in the next step of this research work. Based on the performance analyses of this probable security solution in different aspects for both tiny and heavy devices and in various WSN architectures, the further modification of this probable security solution will be decided.

References

[1] S. H. Jokhio, I. A. Jokhio, and A. H. Kemp, "Light-weight framework for security-sensitive wireless sensor networks applications," IET Wirel. Sens. Syst., vol. 3, no. 4, pp. 298–306, 2013.

[2] A. Bashir and A. H. Mir, "An Energy Efficient and Dynamic Security Protocol for Wireless Sensor Network," Adv. Electron. Syst., pp. 257–261, 2013.

[3] M. Rezvani, A. Ignjatovic, E. Bertino, and S. Jha, "Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks," IEEE Trans. Dependable Secur. Comput., vol. 12, no. 1, pp. 98–110, 2015.

[4] A. Mahmood and A. H. Akbar, "Threats in end to end commercial deployments of Wireless Sensor Networks and their cross layer solution," Information Assurance and Cyber Security (CIACS), pp. 15–22, 2014.

[5] S. Seo, J. Won, S. Sultana, and E. Bertino, "Effective Key Management in Dynamic Wireless Sensor Networks," IEEE Trans. Inf. Forensics Secur., vol. 10, no. 2, pp. 371–383, 2015.

[6] R. Dutta, S. Gupta, and D. Paul, "Energy Efficient Modified SPIN Protocol with High Security in Wireless Sensor Networks Using TOSSIM," Parallel, Distributed and Grid Computing (PDGC), pp. 290–294, 2014.

[7] F. Tong, W. Tang, L. M. Peng, R. Xie, W.-H. Yang, and Y.-C. Kim, "A Node-Grade Based AODV Routing Protocol for Wireless Sensor Network," 2010 Second Int. Conf. Networks Secur. Wirel. Commun. Trust. Comput., vol. 2, pp. 180–183, 2010.

[8] A. Amokrane, Y. Challal, and A. Balla, "A secure web service-based platform for wireless sensor network management and interrogation," 2011 Conf. Netw. Inf. Syst. Secur. SAR-SSI 2011, Proc., 2011.

[9] R. Yin, B. Liu, H. Liu, Y. Li, and M. Dong, "A quantitative fault tolerance evaluation model for topology in wireless sensor networks based on the semi-Markov process," Neurocomputing, vol. 149, pp. 1014-1020, 2015.

[10] S. Yang, J. Liu, C. Fan, X. Zhang, and J. Zou, "A new design of security wireless sensor network using efficient key management scheme," 2010 2nd IEEE Int. Netw. Infrastruct. Digit. Content, pp. 504–508, 2010.

[11] R. Amin and G. P. Biswas, "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," Ad Hoc Networks, vol. 36, pp. 58–80, 2016.

[12] B. Ismail, S. D. Morgera, and S. Ravi, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," IEEE Commun. Surv. TUTORIALS, Accept. Publ., pp. 1–16, 2013.

[13] X. Liu, Y. Shen, S. Li, and F. Chen, "A fingerprint-based user authentication protocol with one-time password for wireless sensor networks," Proc. 2013 Int. Conf. Sens. Netw. Secur. Technol. Priv. Commun. Syst. SNS PCS 2013, pp. 9–12, 2013.

[14] S. K. Udgata, A. Mubeen, J. Chen, and W. Peng, "Wireless sensor network security model using zero knowledge protocol," 2011 IEEE Int. Conf. Commun. ICC 2011, pp. 1–5, 2011.

[15] Q. Liu, L. Liu, X. Kuang, and Y. Wen, "Secure service and management for security-critical wireless sensor network," Proc. - 6th Int. Conf. Innov. Mob. Internet Serv. Ubiquitous Comput. IMIS 2012, pp. 445–449, 2012.

[16] M. H. Ahmed, S. W. Alam, N. Qureshi, and I. Baig, "Security for WSN based on elliptic curve cryptography," in Proceedings - International Conference on Computer Networks and Information Technology, 2011, pp. 75–79.

[17] K. Saleem, N. Fisal, S. Hafizah, and R. A. Rashid, "An intelligent information security mechanism for the network layer of WSN: BIOSARP," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 6694 LNCS, pp. 118–126, 2011.

[18] S. Khanum, M. Usman, and A. Alwabel, "Mobile agent based hierarchical intrusion detection system in wireless sensor networks," Int. J. Comput. Sci. Issues, vol. 9, no. 1, pp. 101–108, 2012.

[19] F. Viani, G. Oliveri, M. Donelli, L. Lizzi, P. Rocca, and A. Massa, "WSN-based solutions for security and surveillance." pp. 1762-1765, 2010.

[20] X. Zhenghong and C. Zhigang, "A Secure Routing Protocol with Intrusion Detection for Clustering Wireless Sensor Networks," pp. 230–233, 2010.

[21] Y. Yao, Y. Fant, S. Security, and E. Engineering, "A Distributed Relay Node Placement Strategy Based on Balanced Network Lifetime for Wireless Sensor Networks," IEEE Int. Confernce Wirel. Commun. Netw. Inormation Secur., pp. 360–360, 2010.

[22] Y. F. Zheng, Z. R. Chen, J. Y. Han, and Z. Li, "A novel based-node level security strategy in wireless sensor network," Proceeding 2012 Int. Conf. Inf. Manag. Innov. Manag. Ind. Eng. ICIII 2012, vol. 1, pp. 507–510, 2012.

[23] J. W. Branch, C. Giannella, B. Szymanski, R. Wolff, and H. Kargupta, "In-network outlier detection in wireless sensor networks," Knowl. Inf. Syst., vol. 34, no. 1, pp. 23–54, 2013.

[24] H. B. Karaman and S. Sagiroglu, "An application based on steganography," Proc. 2012 IEEE/ACM Int. Conf. Adv. Soc. Networks Anal. Mining, ASONAM 2012, pp. 839–843, 2012.

[25] S. Guizani and N. Nasser, "An audio/video crypto Adaptive optical steganography technique," IWCMC 2012 - 8th Int. Wirel. Commun. Mob. Comput. Conf., pp. 1057–1062, 2012.

[26] Z. D. Z. Ding and N. Yamauchi, "An improvement of energy efficient multi-hop time synchronization algorithm in wireless sensor network," Wirel. Commun. Netw. Inf. Secur. (WCNIS), 2010 IEEE Int. Conf., pp. 116–120, 2010.

[27] A. K. Dwivedi and O. P. Vyas, "An Exploratory Study of Experimental Tools for Wireless Sensor Networks," Wirel. Sens. Netw., vol. 03, no. 07, pp. 215–240, 2011.

[28] X. Cai, A. Hu, and R. Liu, "Design of intelligent inductive security system based on wireless sensor network," Energy Procedia, vol. 12, pp. 718–725, 2011.

[29] A. Miyaji, and K. Omote, "Efficient and optimally secure in-network aggregation in wireless sensor networks." pp. 135-149, 2010.

[30] Y. Lim, H.-M. Kim, and S. Kang, "A reliable data delivery mechanism for grid power quality using neural networks in wireless sensor networks," Sensors, vol. 10, no. 10, pp. 9349-9358, 2010.

[31] G. Han, J. Jiang, L. Shu, J. Niu, and H. C. Chao, "Management and applications of trust in Wireless Sensor

Networks: A survey," J. Comput. Syst. Sci., vol. 80, no. 3, pp. 602–617, 2014.
[32] H. W. Ferng, J. Nurhakim, and S. J. Horng, "Key management protocol with end-to-end data security and key revocation for a multi-BS wireless sensor network," Wirel. Networks, vol. 20, no. 4, pp. 625–637, 2014.
[33] J. Liao, B. Zhu, and Y. He, "NLSBT: A localization scheme for underwater 3D acoustic sensor network," NSWCTC 2010 - 2nd Int. Conf. Networks Secur. Wirel. Commun. Trust. Comput., vol. 2, pp. 282–288, 2010.
[34] R. Das and T. Tuithung, "A novel steganography method for image based on Huffman Encoding," Proc. - 2012 3rd Natl. Conf. Emerg. Trends Appl. Comput. Sci. NCETACS-2012, pp. 14–18, 2012.
[35] P. Marwaha and P. Marwaha, "Visual cryptographic steganography in images," 2010 2nd Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2010, 2010.
[36] K. Rangan and T. Vigneswaran, "An Embedded systems approach to monitor green house," Recent Adv. Sp. Technol. Serv. Clim. Chang. 2010 (RSTS CC-2010), pp. 61–65, 2010.
[37] K. Qazanfari and R. Safabakhsh, "A new steganography method which preserves histogram: Generalization of LSB++," Inf. Sci. (Ny)., vol. 277, pp. 90–101, 2014.
[38] M. Momani, S. Challa, and R. Alhmouz, "Bayesian fusion algorithm for inferring trust in wireless sensor networks," J. Networks, vol. 5, no. 7, pp. 815–822, 2010.
[39] E. Aivaloglou and S. Gritzalis, "Hybrid trust and reputation management for sensor networks," Wirel. Networks, vol. 16, no. 5, pp. 1493–1510, 2009.
[40] R. D. Corin, G. Russello, and E. Salvadori, "TinyKey: A light-weight architecture for wireless sensor networks securing real-world applications," 2011 8th Int. Conf. Wirel. On-Demand Netw. Syst. Serv. WONS 2011, pp. 68–75, 2011.
[41] D. Jinwala, D. Patel, and K. Dasgupta, "FlexiSec : A Configurable Link Layer Security Architecture for Wireless Sensor Networks," J. Inf. Assur. Secur., vol. 4, pp. 582–603, 2009.
[42] A. Sahana and I. S. Misra, "Implementation of RSA Security Protocol for Sensor Network Security: Design and Network Lifetime Analysis," Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), pp. 1–5, 2011.
[43] B. Cui and S. J. Yang, "NRE: Suppress Selective Forwarding attacks in Wireless Sensor Networks," 2014 IEEE Conf. Commun. Netw. Secur. CNS 2014, pp. 229–237, 2014.
[44] Yingxu Lai; Yinong Chen; Qichen Zou; Zenghui Liu; Zhen Yang, "Design and analysis on trusted network equipment access authentication protocol", Simulation Modelling Practice and Theory, vol. 51,no., pp. 157-169, Feb. 2015.
[45] Sheetal Kalra; Sandeep K. Sood, "Advanced password based authentication scheme for wireless sensor networks", Journal of Information Security and Applications, vol. 20, no., pp. 37-46, Feb. 2015.
[46] Y. Zhuang; Z. Syed; J. Georgy; N. El-Sheimy, "Autonomous smartphone-based WiFi positioning system by using access points localization and crowdsourcing", Pervasive and Mobile Computing, vol. 18, no., pp.118-136, Apr. 2015.
[47] R. Mai; D.H.N. Nguyen; Le-Ngoc Tho, "Linear Precoding Game for MIMO MAC With Dynamic Access Point Selection", in Wireless Communications Letters, IEEE , vol.4, no.2, pp.153-156, April 2015.
[48] Mai Ruikai; D.H.N. Nguyen; Le-Ngoc Tho, "Joint access point selection and linear precoding game for MIMO multiple-access channels", in Wireless Communications and Networking Conference (WCNC), 2015 IEEE , vol., no., pp.753-758, 9-12 March 2015.
[49] Sahar Hoteit; Stefano Secci, Guy Pujolle; Adam Wolisz; Cezary Ziemlicki; Zbigniew Smoreda, "Mobile data traffic offloading over Passpoint hotspots", Computer Networks, vol. 84, no., pp. 76-93, 19 Jun. 2015.
[50] N. Kumar and S. Kaur, "Performance evaluation of Distance based Angular Clustering Algorithm (DACA) using data aggregation for heterogeneous WSN," 2016 International Conference on Computation of Power, Energy Information and Commuincation (ICCPEIC), Melmaruvathur, Chennai, India, 2016, pp. 097-101.
[51] H. Fakhrey, R. Tiwari, M. Johnston and Y. A. Al-Mathehaji,"The Optimum Design of Location-Dependent Key Management Protocol for a WSN With a Random Selected Cell Reporter," in IEEE Sensors Journal, vol. 16, no. 19, pp. 7217-7226, Oct.1, 2016
[52] M. Li, X. B. Chi, X. C. Jia and J. L. Zhang, "WSN-based efficient monitoring for overhead transmission line in smart grid," 2016 35th Chinese Control Conference (CCC), Chengdu, China, 2016, pp. 8485-8489, 2016.
[53] J. Hou, W. Zeng, G. Wan, J. Zhou and M. Sun, "The analysis and research on the accuracy of WSN node location under the influence of multipath reflection," 2016 35th Chinese Control Conference (CCC), Chengdu, China, 2016, pp. 8352-8355.
[54] L. Mu, X. Qu and Z. Zhou, "SARL: A flexible Simulation Architecture of Range-based Location in WSN," 2016 35th Chinese Control Conference (CCC), Chengdu, China, 2016, pp. 8412-8417.
[55] A. Berger, M. Pichler, D. Ciccarello, P. Priller and A. Springer, "Characterization and adaptive selection of radio channels for reliable and energy-efficient WSN," 2016 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), Doha, Qatar, 2016, pp. 443-448.
[56] Y. Torii, T. Otsuka and T. Ito, "A diversity sensor connection capability WSN for disaster information gathering system," 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS), Okayama, Japan, 2016, pp. 1-6.
[57] D. Jiaying, S. Tianyun, L. Xiaojun and L. Zhi, "Optimal node deployment scheme for WSN-based railway environment monitoring system," 2016 Chinese Control and Decision Conference (CCDC), Yinchuan, 2016, pp. 6529-6534.
[58] A. El Assaf; S. Zaidi; S. Affes; N. Kandil, "Robust ANNs-based WSN Localization in the Presence of Anisotropic Signal Attenuation," in IEEE Wireless Communications Letters , vol.PP, no.99, pp.1-1, 2016.
[59] R. A. Freeda and R. N. Sharmila, "A review of bulk data dissemination protocols for reprogramming in WSN," 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, 2016, pp. 1-4.

Sunil Kumar received the B.Tech. degree in Computer Science & Engineering from Bundelkhand University, Jhansi, India, in 2001 and the M.Tech. degree in Computer Engineering from the Maharshi Dayanand University, Rohtak, India, in 2007. His research interests lie in the area of Computer Networks, Wireless Networks and Cryptography & Network Security. He is currently pursuing Ph.D in Computer Science & Engineering from I. K. Gujral Punjab Technical University, Kapurthala (Punjab), India.

Dr. C. Rama Krishna received B.Tech. from JNTU, Hyderabad (1992) with Distinction, M.Tech. from Cochin University of Science & Technology (1995) with First Division, Cochin, and Ph.D from IIT, Kharagpur (2010) in the area of Mobile Adhoc Networks, and he is Senior Member IEEE. Since 1996, he is working with Department of Computer Science & Engineering, National Institute of Technical Teachers Training & Research, Chandigarh and currently holding the position of Professor and Head of Department (with 20+ years of teaching & research experience). He conducted more than 125 training programmes (Online and Contact mode) of 1 and 2 weeks duration in the upcoming areas of CSE/IT for the faculty of Engineering Colleges and Polytechnics to improve quality of technical education. He is Professor In-charge for Campus-wide Internet Administration, Institute Web Portal and Hardware Maintenance, NCTEL Web Portal for Video Lectures, Go-Green Initiative (paperless office). He is also Liaison Officer for Delhi to finalize training needs and to mobilize teachers to attend various training programmes of NITTTR Chandigarh. His research interests include Computer Networks, Wireless Networks, Cryptography & Cyber Security, and Cloud Computing. He published more than 90 research publications in referred International and National Journals and Conferences. He guided more than 62 Master of Engineering theses in Computer Science and Engineering and he is guiding 8 Ph.D students in the area of wireless networks and cloud computing.

Dr. A. K. Solanki Prof. & Head Information Technology Deptt in Bundelkhand Institute of Engineering & Technology, Jhansi [U.P], India, has obtained his Ph.D degree in Computer Science & Engineering from Bundelkhand University, Jhansi. He has more than 28 years teaching Experience. Prof. Solanki has also appointed as an Executive Committee Member of National Executive Council of Indian Society of Technical Education (ISTE) for three years 2009-2012 for Utter Pradesh and Uttrakhand region. Now currently he is the Section Chairman of Utter Pradesh and Uttrakhand region of Indian Society of Technical Education (ISTE) for three years 2012-2017. He is a members of BOS/RDC in many Universities and also member of Selection & Inspection Committee of AICTE/UPTU and other Universities. He has published a good numbers of International & National research papers in area of Data warehousing, web Mining, Wireless Communication.