Asian Journal of Information Technology 15 (18): 3524-3530, 2016
ISSN: 1682-3915

Techniques for Enhancing Security in Wireless Sensor Networks

Vikas Dhawan and Gurjot Singh Gaba
Department of Electronics and Communication Engineering,
Lovely Professional University, 144411 Jalandhar, India

Abstract: Security of transmitted data is a most important issue in any communication network. While concerning with security of data; attributes such as energy efficiency, low power consumption and less computation time must be taken care of. WSN strives to use those techniques for data security and data aggregation that works on low communication and computation cost because sensor nodes are resource limited. This study deals with performance comparison of different security schemes which claims to work on low computation and communication cost along with the discussion on different security techniques based on data aggregation concept. It has been observed from the analysis that security schemes based on data aggregation concepts are more suitable for WSN than others.

Key words: Data aggregation, data privacy, data security, cryptography, symmetric key, asymmetric key, key management, hash

INTRODUCTION

A Wireless Ssensor Network (WSN) comprises of large number of sensing nodes which performs different kinds of operations like sensing, processing and communicating. When large number of sensor nodes co-operatively monitor large physical environment, they form a Wireless Sensor Network (WSN). Sensor nodes collect information from many applications such as Health Care, Monitoring animal habitats, Military, Tracking at critical facilities and Environmental monitoring. Sensor is defined as a device which produces measurable response to change in any physical condition like temperature, pressure, humidity etc. WSN is defined as set of sensor nodes deployed in certain area for monitoring the events. In WSN, nodes have to perform different types of tasks like sensing, computing and communicating. There exists one Base Station which collects information from different nodes and then computes statistical results and also stores it for further use. In WSN, nodes are deployed in open, hostile and unprotected environment for long term transmissions of data from different source nodes to destination nodes or to base station. It has broadcast nature of transmission due to which it is vulnerable to various types of attacks, such as eavesdropping, snooping, modification, replaying and DOS attack. So, in order to prevent transmitted data or whole network from the adversaries, different types of data security and data privacy techniques are suggested such as cryptography technique, hashing technique. The energy constraint nature of WSN makes implementation of security algorithms very challenging task. The solution for this problem is to maintain a tradeoff between the security of data in WSN and consumption of energy, computing and communication resources in the nodes (Wenqing *et al*., 2006).

Security requirements in WSN:

Time synchronization: In sensor network, time synchronization is an important concern in order to avoid retransmission of message, collisions, etc. which lead to more energy and power consumption, hence leads to reduction in the life span of the network. So, in order to preserve power, proper time synchronization is required, so that individual sensor nodes can turn off their transceivers when not in use.

Robustness and survivability: WSN should be robust against various types of attacks or in case if it is affected by certain attack, it should be able to reduce its impact without affecting rest of the network communication. The damage of the single node must not violate the security of the entire network.

Data confidentiality: Confidentiality is very important concern in Wireless Sensor Network. It is defined as the ability of sensor nodes to protect routed message from the attacker so that it can remain confidential. An authorized node should not reveal any type of information to its neighbor.

Corresponding Author: Vikas Dhawan, Department of Electronics and Communication Engineering,
Lovely Professional University, 144411 Jalandhar, India

Data authentication: It ensures that the given data has been sent by an authorized node. It can be used to prevent many types of active attacks. It uses various types of security keys while sharing data between the receiver and sender side by doing so it basically checks the authenticity of the sender and receiver.

Data integrity: It ensures that the data received by the Cluster Head or any other sensor node is not altered or it has not been tampered or harmed by any attacker node. The integrity of the data is very important in case of WSN because sometime an attacker may add false node which starts generating false data, then in that case, the information may mislead.

Data availability: It basically checks the ability of the nodes for using the resources and the availability of the networks for the message to communicate. Because in any circumstances if base station or cluster head node is not available; then if affects the QOS of the network.

Self-organization: WSN should be designed in such a way so that each node can be independent of each other, so that if any node stops functioning properly, it does not affect entire network. Network should be self-organizing as in case of the cluster head or data aggregating node if it stops functioning then network should be designed in such a way that it can easily adapt the change and change its route.

Data freshness: It is basically used to prevent the replay attacks or spoofing, where attacker can create the routing loops. Due to this, receiver node checks the freshness of the data so as to avoid the unnecessary hearing of these routing loops (Ren *et al*., 2010; Wenqing *et al*., 2006).

Conventional ideologies in cryptography

Cryptography: Cryptography word comes from Greek Origins which means "Secret Writing". It is a technique or art used for hiding or transforming the original content of any message, video or image into some another form to make it difficult to understand by adversaries thereby increasing immunity of system against different types of attacks (Forouzan, 2007). Cryptography primitives are fundamental building blocks for designing security protocols to achieve confidentiality, authentication, integrity and non-repudiation. Cryptography techniques are typically divided into two types: Symmetric and Asymmetric Cryptography (Shim, 2016) which are characterized further along three independent dimensions:

Type of operation used for transforming plaintext to ciphertext: Generally all the encryption algorithms are based on two principles: Former is Substitution, in which each element is mapped into another element. During substitution, addition of new elements may take place. Latter is transposition, in which elements in the plain text are rearranged.

Number of keys used: If system uses single shared secret key for both encryption and decryption, then it is known as symmetric. If system uses two different keys for encryption and decryption then it is known as asymmetric.

The way in which plaintext is processed: It can be done in two ways, stream cipher and block cipher.

Cryptanalysis: It is a technique used by adversaries to crack the code in order to know the original content of the message without knowing the original key. It requires some knowledge of algorithm used along with pairs of plaintext and ciphertext. Attacker tries to exploit the characteristics of algorithm to deduce the key or plaintext (Kahate, 2008; Stallings, 2006).

Key management: In order to maintain security in WSN, key management procedure is a very important factor because keys should be kept out of reach of the adversary. A complete key management scheme should include key generation, key distribution and key updating. Random key pre-distribution scheme is widely considered as the most suitable for WSN (Zhu and Zhan, 2015). In symmetric and asymmetric cryptography techniques, if in any case attacker comes to know about the encryption and decryption key, then it may lead to exploitation of entire network security. So, secure key management should always be carried out to prevent theft of data.

Types of security concerns in WSNs

External security: It protects the data from the outsider's opponent nodes, by assuming all other neighboring nodes as trusted ones.

Internal security: It protects the data from the other participating neighboring nodes. This provides us a privacy of data sensed by different nodes (Bista, 2010).

Algorithms based on symmetric key cryptography: Figure 2 clearly demonstrates that in this type of cryptography, both sender and receiver share a common key for encryption and decryption which is called as secret key. As compare to asymmetric cryptography it consumes less energy, processing and computation

power. Symmetric key algorithm performs faster than asymmetric algorithms (Tajeddine *et al*., 2014). In this, secret key is always evolved out at the end of each interval. The plaintext can be converted into ciphertext by two different ways such as:

Stream cipher: As its name implies, encryption and decryption of data is done bit by bit or byte by byte.

Block cipher: In block ciphers, firstly plaintext can be divided into different set of blocks and then encryption and decryption can be done in the format of one block at a time. They are more secure than the stream cipher (Tajeddine *et al*., 2014). Now, different modes of symmetric algorithms are Cipher Block Chaining Mode Cipher Feedback Mode, Output Feedback Mode, and Counter Mode (Kahate, 2008).

Hashing scheme (μ TESLA) It is mostly assumed that all neighboring nodes are trustworthy. It uses one way hash function for the verification of integrity and for the keys in a MAC algorithm it prefers hash preimages, this scheme works in different time intervals, such as in time interval 1, all the nodes are preloaded with $k_0 = (h(x))^n$ then for all the messages which is going to broadcast within in interval 1, MAC's for them is generated by using $k_1 = (h(x))$ (n-1), here x is secret key held by server. At time interval 2, query server broadcasts k_1 and participating nodes start verifying $h(k_{1)} = (k_0)$ and then this k_1 is also used for the verification of messages received in interval 1 (Ren *et al*., 2010).

Hash function: It is observed from Fig. 1 that in Hash Function, a message of variable length maps into a fix length hashes value or Message Digest. All the Hashing Algorithms involve iterative use of compression function. Hash Function 'H' accepts message 'M' of variable length as input and produces a fixed size hash value:

$$Sh = H(M)$$

A good hash function has a property of converting large set of inputs to fixed length of evenly distributed and apparently random output (Stallings, 2006).

Drawbacks of hashing scheme: Hence this whole process suffers from much delay which may cause DOS attacks, mainly due to:

- Within one time interval, receiver nodes have to buffer all the messages

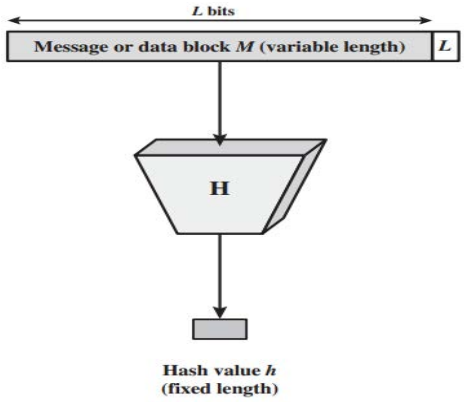

Fig. 1: Cryptography Hash function; h = H (M)

- Receiver nodes are subjected to wormhole attacks. It is cumbersome and costly to implement it as compared to other techniques. To overcome these issues, RC4 and RC5 come into picture (Ren *et al*., 2010)

RC4 (Rivest Cipher 4): It is stream ciphering technique developed by Ron Rivest in 1987. It generates a stream of bits called as keystream which is pseudorandom stream. This keystream is then processed with the plaintext by XORing operation for encryption and even decryption can also happen in this same manner. This overall process includes two steps:

- Initialization of keys
- Stream Generation

But this whole process is much slower, so in order to increase speed of execution RC5 was developed (Kahate, 2008).

RC5 (Rivest Cipher 5): It is a subset of RC4 designed by the Ron Rivest and it is a symmetric block cipher which requires low memory for execution and works faster as well. It provides more security as compared to other symmetric algorithms. The word size, number of 8-bit bytes in the key and number of rounds can be of variable length such as the word size can be of (16, 32, 64) bits, number of rounds can be (0-2040) bits, number of octets in the key can be (0-2040) bits. Once These are pre-initialized values which will never change throughout particular execution of cryptographic algorithm. RC5 is also renowned as RC5-w/r/b where 'w' stands for word size, 'r' stands for number of rounds and 'b' stands for number of octets in the key.

Drawbacks in RC5:

- Size of the key which affect the computational overhead and memory requirements
- Size of the MAC (Message Authentication Code), since it is added into the message which leads to increase in the message byte count. Since these two factors are chosen by the administrator of the network, so it is always suggested to built a stronger algorithm which is hard to break. Its performance can be more enhanced by using different modes such as RC5 block cipher, RC5-CBC, RC5-CBC-Pad, RC5-CTS (Kahate, 2008; Tajeddine *et al*., 2014)

Drawbacks in symmetric keys:

- The worst drawback is that it uses only one single secret key, so in that case if adversaries are able to know it then they can destroy the CIA attribute of the whole network
- The symmetric key algorithm cannot perform well in case of large scale WSNs.

MATERIALS AND MEHTODS

Algorithms based on asymmetric key cryptography: It is clearly observed from Fig. 2 that in Asymmetric Cryptography, we use two different keys which are mathematically linked, one is used for encryption purpose and other one is used for decryption. Private Key remains secret and is not shared with any other node, whereas public key is known to every user. Public key remains same for the fixed period of time in WSNs to save computation energy, whereas private key can be updated after each interval (Tajeddine *et al*., 2014). It provides a more flexible and simple interface without the need for pair wise sharing. It is considered to be too computationally expensive for small wireless devices (Shim, 2016).

The certification-based authentication scheme: In this scheme, each user uses a digital signature scheme such as RSA, whenever he broadcast any message. In this, destination node or query server also have their own public/private keys and it serves as certificate issuing authority because it issues a public key certificate to each user, this certificate consists of User ID, Public Key User ID, Certification expiry time and signatures, when any user broadcast its message, it has to face two verification steps, i.e., Certificate verification and Signature verification.

Drawbacks: In CBA scheme, user revocation and certification revocation persists and in order to support this, there must be a Certification Revocation List (CRL) at all the time during communication. This would require large memory for storing CRL which effect the memory requirements of WSNs. Moreover, verification of signatures has been done two times which makes the whole process slow (Ren *et al*., 2010).

Merkle hash tree scheme: It is highly efficient as compare to certification approach in terms of storage factor. The query server collects all the public keys of other participating nodes in order to create merkle hash tree which later constructs N leaves corresponding to each user, each user has binding between public key and User ID. The value of idle level node derivers from the base nodes and from them we are able to find root node denoted as (hr), 'hr' should be signed by the query server to prove its authenticity, if it is broadcasted at the time of network operation. At the same time, each node obtains its AAI according to its location in the merkle hash tree. In this scheme, verification of broadcast message is a chain process including several hash operations with final value equal to 'hr', if it is not equal to 'hr' then it indicates the invalidity of corresponding public key. Further, it also verifies the signature using public key User ID, if any revocation exists, then sink will update the tree and send information about new root node 'hr' and 'AAI' to all other users (Ren *et al*., 2010).

Drawbacks: This scheme tried to reduce the revocation problem but behaved inefficiently when number of users gets increased because sensor nodes have to memorize information about all other leaves of the merkle hash tree.

ID-based authentication scheme: It is more efficient as compared to merkle hash tree scheme because in this scheme sensor node only need to memorize about revoke User's ID and it also uses automatic public key update scheme. The time is divided into different intervals for uniform updations. User gets its private key from sink which is valid only for one-time interval. New private key is issued at the beginning of each interval, where as it gets public key under an ID-Based Signature Scheme (Intanagonwiwat *et al*., 2000). Now in case of any revocation, users have to memorize only revoked User's ID which is broadcasted by sink, valid only within one-time interval and dumps afterwards. Thus, this scheme eliminates any requirement of certificate verification and also reduces storage problem as we seen in first two schemes (Ren *et al*., 2010).

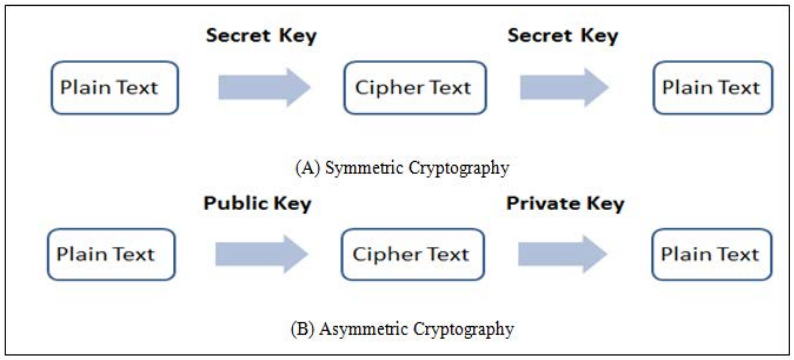

Fig. 2: Types of cryptography scheme

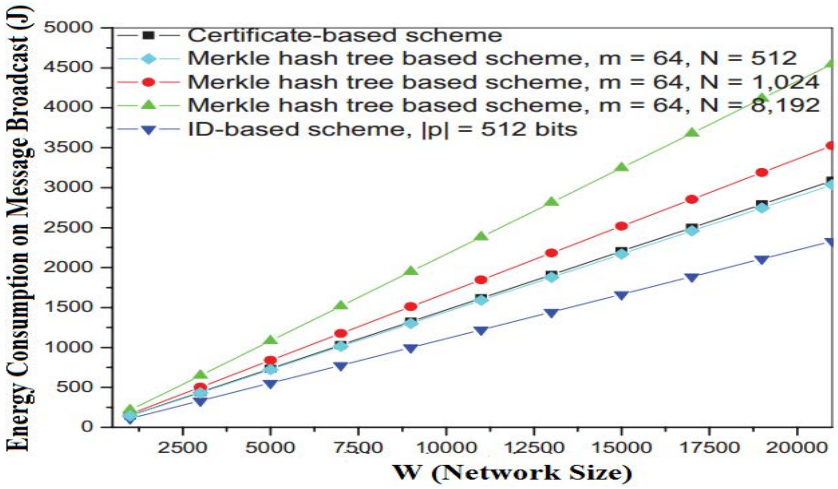

Fig. 3: Energy consumption on message broadcast

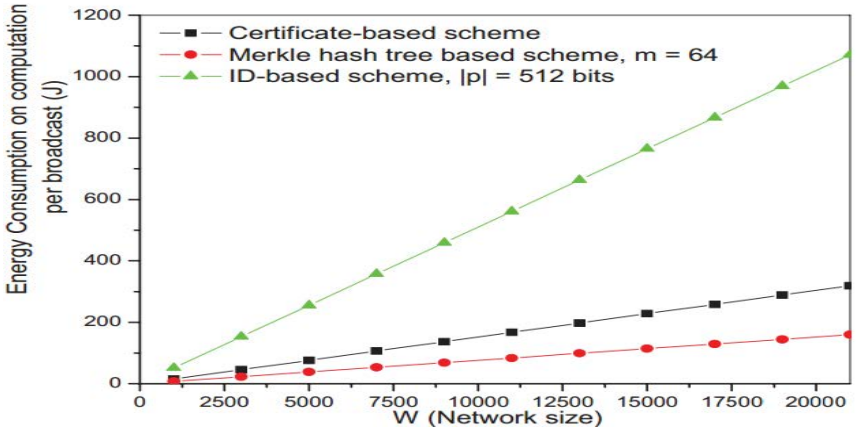

Fig. 4: Energy consumption on computation

It is clearly seen from Fig. 3 and 4 that energy consumption on message broadcast and energy consumption on computation in case of Merkle Hash Tree (MHT) Scheme with fewer users is quite low as compared to other techniques.

Schemes based on data aggregation concept: Since, in WSN, power available to nodes, bandwidth, memory size and processing speed is limited, so in order to use these features wisely, data aggregation schemes are considered to be the appropriate choice, because instead of sending all raw data only required data is sent under the aegis of this scheme. It also reduces number of participating nodes, data packet size and number of transmissions. Based upon that, there are two types of security algorithms such as end to end and hop by hop but by using end to end security algorithms one can get more security because in case of Hop by Hop, data has to be decrypted first due to which neighboring nodes might be able to listen some kind of private data. This does not happen in case of End to End. In this strategy, initially cipher text is added and then digital signatures and then public keys and afterwards node send it to the aggregator. Different aggregation schemes are:

Secure Hierarchical Data Aggregation algorithm (SHDA): WSN is organized in the form of tree, then instead of sending sensed data directly to the sink, use of different cluster heads or aggregators have been suggested, each node transmits sensed data by encrypting it using ECEG (Elliptic Curve Elgamal Algorithm) and then sign it by using modern version of ECEG which is ECDSA (Elliptic Curve Digital Signature Algorithm). Since, ECEG is homomorphic encryption scheme, it allows parent node to aggregate encrypted data, signatures and public keys of different child nodes at base station. Table 1 shows time taken and energy consumed during various operations such as Encryption, Signing and Cipher text Addition, Signature Addition and Public-Key Addition (Kumar and Madria, 2010).

PDA (Privacy-Preserving Data Aggregation): It is further divided into two categories:

CPDA (Cluster Based Private Data Aggregation): In this scheme, cluster formation occurs randomly in order to create aggregation tree. It uses the concept of additive property of polynomials to get desired final value. It also guarantees for the privacy of data values of sensor nodes from each other. Firstly, each user node customize its data into polynomial form, then all sensor nodes present within one cluster exchange their encrypted data, then each nodes present in the cluster use additive property of polynomial for assembling its own data and data receiving from other nodes and send it to their respective cluster heads. Then CH's computes the final aggregated value by using matrix inverse technique and send it to the base station through the routing tree (Bista *et al*., 2010).

Table 1: Performance analysis of SHDA algorithm

	Qos and lifetime indicator	
Operations	Execution time (m sec)	Energy consumed (mj)
Encryption	117905.1	2829.72
Signing	38884.4	933.22
Cipher text addition	317.3	7.61
Signature addition	0.183	0.004
Public key addition	160.5	3.85

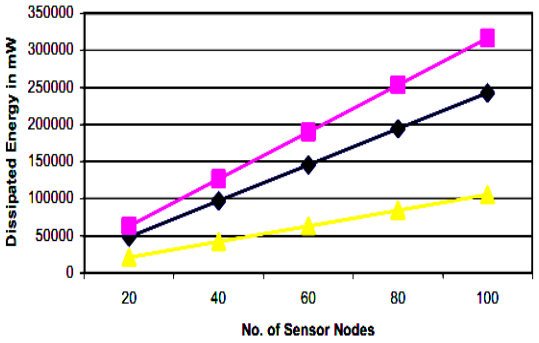

Fig. 5: Energy consumption by the generated messages

SMART (Slice-Mix-Aggregate): In order to hide the data or to protect it from the neighboring nodes, it uses the concept of slicing by customizing the original data into different pieces and sending it to its neighboring nodes which deduce some aggregate value, after receiving data slices from all other participating neighboring nodes (Bista *et al*., 2010).

A New Private Data Aggregation scheme (NPDA): Since, both CPDA and SMART techniques suffers from high communication cost due to unnecessary traffic and high computing cost due to expensive computation techniques, so in order to reduce these factors a new technique has been developed in which additive property of complex number has been used instead of additive property of polynomial, in this both real and imaginary parts have been assigned to each user node. It is clear from Fig. 5 that by using additive property of complex number energy consumption by the generated messages has been reduced to great extent (Bista *et al*., 2010).

RESULTS AND DISCUSSION

The performance of different techniques has been compared on the basis of various parameters such as data security, data privacy, cost factor, execution time, number of keys used in the scheme, digital signature and data aggregation concept. Table 2 shows evaluation statistics of various parameters which make it clear that New scheme (NPDA) proposed by researcher in Bista *et al*.

Table 2: Performance analysis of conventional techniques

Type of techniques	Schemes	Data security	Data privacy	Cost factor	Execution time	Ni. of keys used	Digital signature	Data aggregation
Symmetric key Cryptography	Hashing Scheme	Yes	No	High	More	1	No	No
	RC4	Yes	No	Medium	Moderate	1	No	No
	RC5	Yes	No	Low	Less	1	No	No
Asymmetric key Cryptography	Certification Based	Yes	No	High	More	2	Yes	No
	MHT	Yes	No	Medium	Moderate	2	No	No
	ID Based	Yes	No	Low	Less	2	Yes	No
Based on data aggregation concept	Secure hierarchical approach	Yes	No	High	More	-	Yes	Yes
	CPDA	Yes	Yes	Medium	Less	-	No	Yes
	SMART	Yes	Yes	Medium	Less	-	No	Yes
	NPDA	Yes	Yes	Least	Least	-	No	Yes

(2010) is best suitable as compared to other techniques in all aspects also from Fig. 5, it can be seen clearly seen that energy consumption by the generated messages is quite low in case of NPDA. So, it is found to be the best technique for providing security/aggregation in resource constraint environments such as WSN.

CONCLUSION

The performance of different techniques is recorded on the basis of various parameters. Results points out to the significance of the NPDA scheme which comes out to be more efficient in terms of all aspects as compared to other techniques. Therefore, it is concluded that security schemes based on Data aggregation principle performs well as compared to other schemes because they can manage the tradeoff between security of data in WSN and consumption of energy, computing and communication resources in the nodes in a much better way.

REFERENCES

Bista, R., K.H. Dae and J.W. Chang, 2010. A new private data aggregation scheme for wireless sensor networks. Proceedings of the 2010 IEEE 10th International Conference on Computer and Information Technology, June 29-July 1, 2010, University of Bradford Bradford, United Kingdom, ISBN: 978-1-4244-7547-6, pp: 273-280.

Forouzan, B., 2007. Cryptography and Network Security. McGraw-Hill, New Delhi, India,.

Intanagonwiwat, C., R. Govindan and D. Estrin, 2000. Directed diffusion: A scalable and robust communication paradigm for sensor networks. Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, August 6-11, 2000, Boston, MA., USA., pp: 56-67.

Kahate, A., 2008. Cryptography and Network Security. McGraw-Hill, New Delhi, India,.

Kumar, V. and S. Madria, 2010. Performance analysis of secure hierarchical data aggregation in wireless sensor networks. Proceedings of the 2010 11th International Conference on Mobile Data Management, IEEE, Kansas, USA., ISBN: 978-1-4244-7075-4, pp: 299 300-10.1109/MDM.2010.37.

Ren, K., W. Lou, K. Zeng and P.J. Moran, 2010. On broadcast authentication in wireless sensor networks. IEEE Trans. Wireless Communi., 6: 4136-4144.

Shim, K.A., 2016. A survey of public-key cryptographic primitives in wireless sensor networks. IEEE. Commun. Surv. Tutorials, 18: 577-601.

Stallings, W., 2006. Cryptography and Network Security: Principles and Practices. 3rd Edn., Pearson Education India, New Dehli, India, ISBN: 978-1-25-902988-2, Pages: 492.

Tajeddine, A., A. Kayssi, A. Chehab and I. Elhajj, 2014. Authentication schemes for wireless sensor networks. Proceedings of the 2014 17th IEEE Mediterranean Electrotechnical Conference on MELECON, April 13-16, 2014, IEEE, Beirut, Lebanon, pp: 367-372.

Wenqing, C., L. Weimin, T. Yunmeng and Y. Zongkai, 2006. Research on the security in wireless sensor network. Asia J. Inform. Technol., 5: 339-345.

Zhu, L. and Z. Zhan, 2015. A random key management scheme for heterogeneous wireless sensor network. Proceedings of the 2015 International Conference on Cyber Security of Smart Cities Industrial Control System and Communications (SSIC), August 5-7, 2015, IEEE, New York, USA., pp: 1-5.