Indian Journal of Science and Technology, *Vol 9(32), 10.17485/ijst/2016/v9i32/100725, August 2016*

ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Efficient Approach for Securing Message Communication in Wireless Sensor Networks from Node Clone Attack

Vandana Mohindru* and Yashwant Singh

Department of Computer Science and Engineering, Jaypee University of Information, Technology, Waknaghat 173234, Solan, India; vandanamohindru@gmail.com, yashu_want@yahoo.com

Abstract

Objectives: Security is a very decisive factor for Wireless Sensor Networks because of ever growing popularity in the tangible world. These types of resource constrained network suffers from physical attack, i.e. Node clone attack. **Methods/ Statistical Analysis**: In Node clone attack an attacker capture a node, modify it and replicate clone node in WSNs. The main motive of these clone nodes to obtain mastery over the whole network and to aggravate various inside attacks against sensor networks. The message during communication from the one legitimate node to another legitimate node is also not secure thus altered by the attacker. **Findings:** In this paper, we propose an efficient algorithm for securing message communication in Wireless Sensor Networks (WSNs) from node clone attack. This algorithm makes use of the hybrid cryptography technique which consist of Advanced Encryption Standard (AES) and Elliptical Curve Cryptography (ECC) and lightweight hash function. In this algorithm, AES algorithm encrypts the message and digital signature whereas ECC algorithm encrypts the private key and generates digital signature. The lightweight hash function produces small and fixed size hash digest from the message. The analysis of the proposed algorithm is performed on the ground of parameters like computational overhead, communication overhead, storage overhead and high security level. **Application/Improvements:** The proposed algorithm authenticate message during communication with confidentiality. The analysis indicates that the suggested algorithm is suited for energy constrained sensor networks.

Keywords: Wireless Sensor Network, Node Clone Attack, AES, ECC, Hybrid Cryptography.

1. Introduction

In the late years, Wireless sensor networks becoming popular due to the low-cost, unattended nature and the capability of self-organization of sensor nodes. A Wireless Sensor Networks comprised of resource constrained sensor nodes that are densely deployed in a unattended environment[1]. The sensor nodes collect data from the physical phenomena which occur in the environment, process it and transmit the sensed data via wireless signals to the base station. A base station is power rich node among all sensor nodes in WSNs[2]. Sensor nodes are typically categorized by low-cost, low-power, multifunctional, low bandwidth, small memory sizes and limited energy. Due to these characteristics WSN ensures a broad range of applications in areas such as military, health, environment, commercial and agriculture. Consequently, securing these kind of network becomes a most critical task[3]. The security of WSNs can be accomplished by meeting the security objectives i.e. Availability, Authorization, Authentication, Confidentiality, Integrity, Non repudiation and Freshness[4,5]. The sensor networks are generally situated in isolated environment and left unattended, so they should be equipped with security mechanisms to defend against attacks such as physical tampering, eavesdropping, node capture, denial of service, wormhole, Sybil attack etc[6,7]. Among stall physical attacks to wireless sensor networks, the node clone attack is a serious and precarious one. In Node Clone Attack the sensor network nodes are physically captured and compromised by an

**Author for correspondence*

attacker. Attacker then extracts all secret information (Id, Keys, etc.) from the node and replicate the large numbers of clones of captured node throughout the wireless sensor network[8]. These cloned nodes seem to be legitimate nodes therefore they can participate in the network communication and get total control over the sensor network which in turn result in WSNs disruption. From the security perspective, the node clone attack is extremely harmful and it intensifies most of the internal attacks against sensor networks like Denial of service (DoS), Wormhole, Sybil and many more[9]. For Example as shown in Figure 1, attacker compromise a sensor node say A, fabricate it and generate number of clone of node A. Then attacker puts many clones of node A nearby node B. Node B may take these clone nodes as its new neighbors and they take part in the network tasks in the same manner as genuine nodes. So, cloned nodes can launch a variety of attacks and create inconsistency within the sensor network.

Once the clone entered into the wireless sensor network it will eavesdrop the message transmitted between the genuine sender and receiver sensor nodes, then modify the message and insert false message into the network which will go to the receiving sensor node. The receiving sensor node gets the unauthorized message from the sender node which is modified by the clone node. Therefore, different security measures are too taken in order to secure message communication between the sensor nodes and secure network from the effect of the node clone attack. Cryptography is one of the primary techniques used for securing information while message communication[10]. Cryptography techniques provide confidentiality, authentication, and integrity of the message as well as of sensor nodes in WSNs. There are two types of cryptographic techniques which are mostly used i.e. symmetric cryptography and asymmetric cryptography.

Symmetric Cryptography: In this, a single key is used for both the encryption and decryption[11] e.g. DES, AES, RC4, etc. Symmetric cryptography is also known as secret key or private key cryptography. This cryptography techniques are fast and efficient, low resource consuming, low computation cost, moderately secured and have high storage overhead[12].

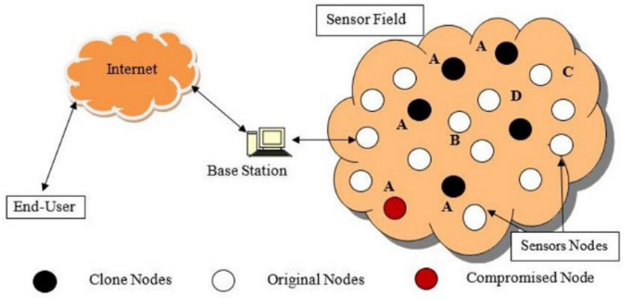

Figure1. WSN with node clone attack scenario

Asymmetric Cryptography: In this, one key (public) is utilized for encryption and another key (private) is employed for decryption e.g. RSA, ECC, etc. Asymmetric cryptography is also known as public key cryptography[13]. These cryptography techniques are more tedious, high resource consuming, high computation cost, highly secured but have low memory overhead[14]. Beside these two cryptography technique hybrid cryptography is also widely used for securing the wireless sensor network from node clone attack.

Hybrid Cryptography: Hybrid cryptography is a blend of symmetric and asymmetric cryptography[15]. The symmetric cryptography technique provides a suitable amount of security, but maintenance of keys is difficult. On the other hand, in asymmetric algorithms maintenance of keys is easier, but they offer a lesser level of security. The limitations of symmetric-key cryptographic techniques were resolved by the asymmetric cryptographic technique. Therefore when combined form of these cryptography techniques are used in the WSNs, they out come with a new technique which is more resilient against the attacks and hence retain the high degree of security[16,17] e.g. AES and ECC, AES and RSA, RC4 and ECC. In this paper, we propose an algorithm which employs the hybrid cryptography technique with lightweight hash function. The paper is organized as follows: Section 2 discussed the related work. In Section 3 we introduced the proposed algorithm for securing the message communication within WSNs from node clone attack. Section 4 presents the analysis of proposed algorithm. At last, we conclude our work in section 5.

2. Related Work

Various detection methods has been previously developed in order to protect wireless sensor networks from node clone attack. Detection methods for node clone attack categorized into two categories: centralized detection and distributed detection. In centralized detection method all nodes send data to a central base station, where base station makes judgments related to node clone. Centralized detection methods include base station based, SET[18], random key predistribution[19], etc. All these centralized detection suffers from central failure of base station. Therefore, distributed detection methods come into existence in which all sensor nodes supportively process information and identify the node clone in a distributed manner. Distributed detection methods include node-to-network broadcasting, randomized multicast, Randomized Efficient Distributed detection (RED) protocol[20], DHT[21,22], XED[23], etc. All these distributed detection methods have their merits and demerits in terms of computational overhead, communication overhead, storage overhead and security level. Beside these detection methods few works has been done to prevent wireless sensor network from node clone attack. Prevention methods integrally prohibit cloned nodes to join the sensor network. Location-based keys method developed to defend against node clone attack[24] in which identity-based cryptography is used. Also various cryptography techniques were developed for securing sensor nodes and message communication in sensor networks. In[25] Byte-oriented Substitution-Permutation Network (BSPN), was proposed for attainment of energy efficiency and security by using symmetric key cryptographic algorithms in WSNs. End-to-End secure communication[26] technique was introduced to check the authentication and to encrypt the messages using IPv6 mechanisms. Also, identity-based signature scheme developed[27] to provide multi-time usage of the offline storage. Hybrid cryptography algorithms are widely used now days for securing WSNs. Hybrid cryptography algorithm comprises of symmetric as well as asymmetric cryptography algorithms, thus they provide much more security to sensor networks. In[28] a hybrid authenticated key agreement with rekeying proposed which combines Symmetric and Elliptic Curve Cryptography. In[29] hybrid encryption scheme was described for secure key exchange and node authentication which is a blend of AES and ECC algorithms. A unique polynomial based Q composite random[30] scheme was establish for generating triple key among communicating nodes in a network. This scheme combines the strength of Q-Composite Key Generation method with the Polynomial Pool-Based method for secure communication between wireless sensor nodes. Two secure data transmission[31] technique was proposed by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/ Offline digital Signature (IBOOS) scheme, respectively.

All the mentioned methods uses the cryptography approach for securing the sensor network which suitable for energy constrained WSN. But our proposed algorithm provides much more security against node clone attack and consumes less energy.

3. Proposed Algorithm

The prime motive of our proposed algorithm is to secure message communication in energy-starved networks i.e. WSNs. The algorithm makes use of the hybrid cryptography algorithm along with a lightweight hash function. Our algorithm claim to offer high level of security, consumes less energy and low computational overhead.

3.1 Background

The proposed algorithm consists of:

Symmetric cryptography algorithm –Advanced Encryption Standard (AES) make use of block cipher with a block length of 128 bits, key length of 128 bits and encryption process consists of 10 rounds of processing[32]. Each round of processing includes one single-byte substitution step, a shift row step, a column-wise mixing step, and the addition of the round key[33].

Asymmetric cryptography algorithm -Elliptical Curve Cryptography (ECC) provide security at much smaller key sizes. ECC is typically useful in applications where memory, bandwidth, and computational power are limited[34]. ECC uses various properties of the points on the curve, and various functions on them. Therefore, in encryption main task is to find a way to turn information m into a point P on a curve E[35].

Lightweight hash algorithm - A cryptographic hash function takes a variable-length of data as input and yields in a fixed-size hash value called hash digest. The hash function is utilized in a wide range of security applications like securing node and message in networks. Lightweight hash algorithm includes block size of 512 bits and result in final hash digest of 24-bit. Lightweight is called because it work on bits and make use of low overhead operations like MOD, XOR, etc.

3.2 Assumptions

3.2.1 Network Model

We consider stationary homogeneous sensor networks, in which a Base Station (BS) which is a powerful node that gather data from sensor nodes in WSN. The network consists of N number of resource constrained sensors in the network that can be compromised and physically captured. The base station has information, i.e. ID, location, etc. related to each sensor node in WSN. Each node within WSN maintain information related to unique ID, location, neighbor list (id, location) corresponding to each 1-hop neighbors.

3.2.2 Security Model

We consider sensors nodes which are not tamper-resistant. Attacker compromises the sensor nodes, which in turn releases all its security information to it. Subsequently, the attacker can start replicating the node, and pass around the clones throughout the WSNs. The clone node can easily take part in the network functioning in the same manner as the genuine node. The cloned nodes are under the command of the attacker, and therefore can launch various internal attacks afterward.

3.3 Algorithm

Step 1: Sensor node A want to send the message to node B. Therefore, sensor node a message first goes to Lightweight Hash function module which results in a hash digest H as shown in Figure 2.
Step 2: Pseudo random generator generates the Session key (K_s).
Step 3: Now hash digest H is passing to ECC encryption module to generated digital signature using sender's private key. Also, ECC encryption module encrypts the private key K_{AES}.
Step 4: The generated digital signature and plain text message are forward to AES encryption module which further result in the data cipher text signature.
Step 5: Now this complete cipher text is transmitted through WSN to sensor node B.
Step 6: The receiver sensor node B, receives the cipher text and uses his private key to decrypt the AES key i.e. K_{AES} using the ECC decryption module as shown in Figure 3.
Step 7: Then, decryption of data cipher text and signature cipher is done by AES decryption module by using K_{AES}.
Pace 8: By using the sender's public key and ECC decryption module verification of the signature is done and resultant H' is generated.
Step 9: Now plaintext goes to Lightweight Hash function module which result in H hash digest.
Step 10: At last, comparing the values of H with H' we find if the values of H and H' are same then the message is authenticated else message is modified by the clone node.

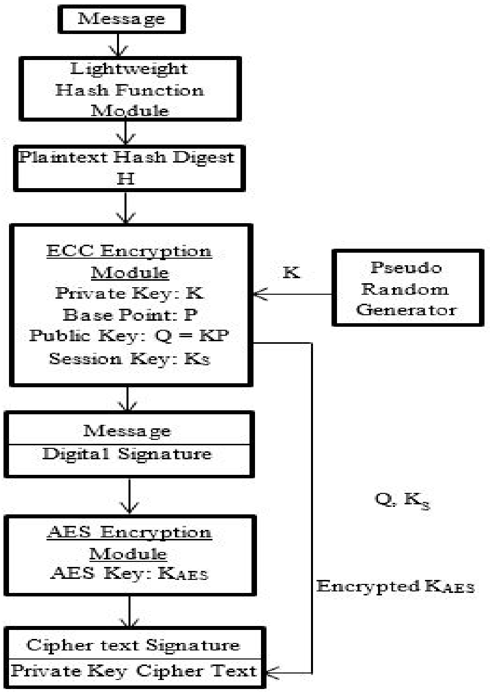

Figure 2. Sender node A

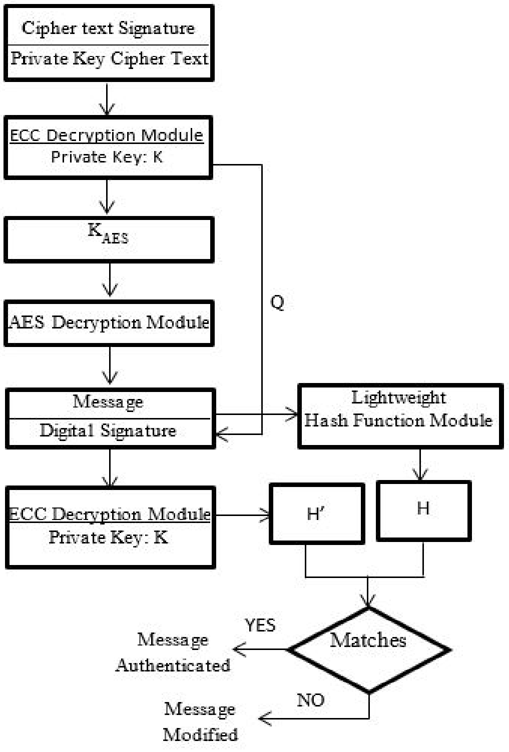

Figure 3. Receiver Node B

From the algorithm we obtain the authenticated message through a hostile environment. If at the last step, H and H' values are not matched then receiving node sends the revocation message to the sender node and also to all the other nodes within the WSN that message is corrupted or clone node is present. Then, the base station sends the alert message within the sensor network to discard the clone node.

4. Analysis of Proposed Algorithm

The effectiveness of any cryptographic algorithm depends on mainly two factors, one is the encryption / decryption methods and another key is used. The proposed algorithm uses the hybrid approach, including the AES and ECC algorithms which make the proposed algorithm more robust and cannot be easily attacked by the clone attack. The message and digital signature are encrypted by AES algorithm which is faster than ECC algorithm and the private key of AES is encrypted with ECC algorithms which are more complicated and secure. Therefore, we have the advantages of AES algorithm, i.e. low communication overhead and low computational overhead and the advantages of ECC algorithm, i.e. high security and low storage overhead in our proposed algorithm. In addition, lightweight hash function is also used for message authentication and message integrity.

The following metrics are used to measure the performance of proposed algorithm:

a. **Communication overhead:** Communication overhead is calculated by the amount of energy consumed for transmitting one byte of data. According to Mica2 specification for AT Mega 128 processor, energy consumption required for transmitting one byte of data is 16.25 μJ and for receiving one byte of data is 12.25 μJ. The proposed consume less energy while message communication and therefore have the lower communication overhead.
b. **Computational overhead:** Computational overhead is calculated by the amount of energy needed during encryption/ decryption process and hash function calculation. The energy required per clock cycle is 3.2nJ or 0.0032μJ. The proposed algorithm computational overhead is less as compared to the other encryption algorithms.
c. **Storage overhead:** Storage overhead is calculated by the amount of data stored in a memory of the sensor nodes. In proposed algorithm we use the lightweight hash function which converts the message into bits which require less amount of memory storage. Also encryption process makes the size of message and key small. Therefore, the proposed algorithm is acceptable by WSNs.

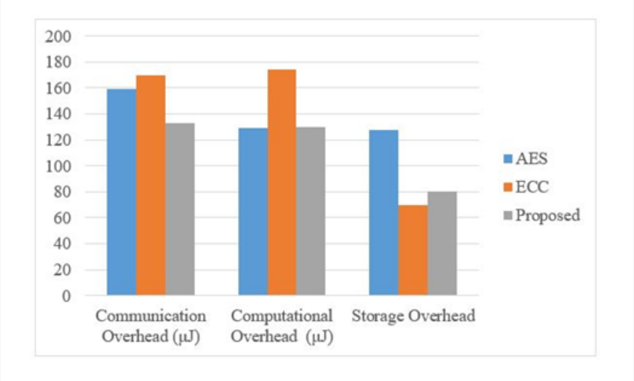

Figure 4. Comparison Chart

d. **Security level:** The prime requirement of any WSNs algorithm is high security by achieving security objectives i.e. authentication, confidentiality, integrity. The propose algorithm provides strong security by applying AES encryption process and hash function. ECC algorithm provides double security to secret key.
e. **Total energy consumed:** The total energy consumed by the sensor node is the sum of energy consumed during message communication and computation.

Comparative analysis of the proposed algorithm with AES and ECC is depicted in Figure 4. Thus from the discussion, it can analyze that the proposed algorithm is designed for energy constrained networks, i.e. WSNs which provides a high degree of security, low computational overhead and low communication over head. Also, it ensures authentication as well as integrity of the message.

5. Conclusion

In this paper, an efficient algorithm is proposed to secure message from being modified by the node clone attack. The algorithm first uses the lightweight hash function which results in a fixed size hash digest which is of modest size. Then the AES algorithm is used for message and digital signature encryption and ECC algorithm is utilized for secret key encryption. By using the hybrid cryptography algorithm the sensor network security increases double times in terms of authentication, confidentiality. The modified messages (modified by clone attack)can be found out easily by using this proposed algorithm because single bit alteration will result in drastic changes in modified message. From the performance analysis, it can be reasoned that the proposed algorithm provides low computational overhead, low communication overhead, low memory overhead, consume less energy and attain a high level of security. The comparative performance also shows our scheme's energy efficient. As the future extension, this algorithm would be simulated using the simulator and can be applied to real world application to check the performance.

6. References

1. Yick J, Mukherjee B, Ghosal D. Wireless sensor network survey, Journal of Computer Networks. 2008 Aug; 52(12):2292-2330.
2. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor networks: a survey. Journal of Computer networks. 2002; 38(4):393-422.
3. Al Ameen M, Liu J, Kwak K. Security and privacy issues in wireless sensor networks for healthcare applications, Journal of Medical Systems. 2012 Feb; 36(1):93-101.
4. Zhou Y, Fang Y, Zhang Y. Securing wireless sensor networks: a survey. Journal of Communications Surveys and Tutorials, IEEE.2008 Sep; 10(3):6-28.
5. Ahmad Salehi S, Razzaque MA, Naraei P, Farrokhtala A. Security in Wireless Sensor Networks: Issues and Challenges, Proceeding of the 2013 IEEE International Conference on Space Science and Communication (IconSpace), Malaysia. 2013 Jul, 356-360.
6. Blilat A, Bouayad A, el houda Chaoui N, Ghazi ME. Wireless sensor network: Security challenges. Proceeding of the JNS2, Morocco. 2012, 68-72.
7. Lupu TG, Rudas I, Demiralp M, Mastorakis N. Main types of attacks in wireless sensor networks. Proceedings of the 9th WSEAS International Conference on Recent Advances in Computer Engineering. 2009 Sep, 180-185.
8. Parno B, Perrig A, Gligor V. Distributed detection of node replication attacks in sensor networks. Proceedings of the IEEE Symposium on Security and Privacy (S&P'05), California. 2005 May, 49-63.
9. Zhu WT, Zhou J, Deng RH, Bao F. Detecting node replication attacks in wireless sensor networks: a survey. Journal of Network and Computer Applications. 2012 May; 35(3):1022-1034.
10. Stallings W. Cryptography and network security: principles and practices, 5th(edn) Prentice-Hall. 2013.
11. Hayouni H, Hamdi M, Kim TH. A Survey on Encryption Schemes in Wireless Sensor Networks. Proceedings of the 7th International Conference on Advanced Software Engineering and Its Applications (ASEA), China.2014 Dec, 39-43.
12. Si L, Ji Z, Wang Z. RETRACTED: The Application of Symmetric Key Cryptographic Algorithms in Wireless Sensor Networks, Physics. Procedia of International Conference on Solid State Devices and Materials Science, Macao. 2012 Apr, 25, 552-559.
13. Goodman J, Chandrakasan AP. An energy-efficient reconfigurable public-key cryptography processor. IEEE Journal of Solid-State Circuits. 2001 Nov; 36(11):1808-1820.
14. Wander AS, Gura N, Eberle H, Gupta V, Shantz SC. Energy analysis of public-key cryptography for wireless sensor networks. Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications (PerCom), Hawaii. 2005 Mar, 324-328.
15. Li X, Chen J, Qin D, Wan W. Research and Realization based on hybrid encryption algorithm of improved AES and ECC. Proceedings of the International Conference on Audio Language and Image Processing (ICALIP), Shanghai. 2010 Nov, 396-400.
16. Ganesh AR, Manikandan N, Sethu SP, Sundararajan R, Pargunarajan K. An improved AES-ECC hybrid encryption scheme for secure communication in cooperative diversity based Wireless Sensor Networks. Proceedings of the International Conference on Recent Trends in Information Technology (ICRTIT), India. 2011 Jun, 1209-1214.
17. Krikis G, Antonopoulos C, Voros N. Design and implementation of efficient reconfigurable cipher algorithms for wireless sensor networks, Proceedings of the 11th IEEE International Conference Industrial Informatics (INDIN), Bochum.2013 Jul, 821-826.
18. Choi H, Zhu S, La Porta TF. SET: Detecting node clones in sensor networks. Security and Privacy in Communications Networks and the Workshops. Proceedings of the Third International Conference on Security and Privacy in Communication Networks and the Workshops (SecureComm), France. 2007 Sep, 341-350.
19. Brooks R, Govindaraju PY, Pirretti M, Vijaykrishnan N, Kandemir MT. On the detection of clones in sensor networks using random key predistribution. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews). 2007 Nov; 37(6):1246-1258.
20. Conti M, Di Pietro R, Mancini LV, Mei A. A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks. Proceedings of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing, Canada. 2007 Sep, 80-89.
21. Li Z, Gong G. DHT-based detection of node clone in wireless sensor networks. Ad Hoc Networks. 2009 Sep, 28, 240-255.

22. Li Z, Gong G. On the node clone detection in wireless sensor networks. IEEE/ACM Transactions on Networking. 2013 Dec; 21(6):1799-1811.
23. Yu C M, Lu C S, Kuo S Y. Mobile sensor network resilient against node replication attacks, Proceedings of the 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON'08), San Francisco. 2008 Jun, 597-599.
24. Zhang Y, Liu W, Lou W, Fang Y. Location-based compromise-tolerant security mechanisms for wireless sensor networks. IEEE Journal on Selected Areas in Communications. 2006 Feb; 24(2):247-260.
25. Zhang X, Heys HM, Li C. Energy efficiency of symmetric key cryptographic algorithms in wireless sensor networks, Proceedings of the 25th Biennial Symposium on Communications (QBSC), Kingston. 2010 May, 168-172.
26. Raza S, Duquennoy S, Chung T, Voigt T, Roedig U. Securing communication in 6LoWPAN with compressed IPsec. Proceedings of the International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS). 2011 Jun, 1-8.
27. Liu JK, Baek J, Zhou J, Yang Y, Wong JW. Efficient online/offline identity-based signature for wireless sensor network. International Journal of Information Security. 2010Aug; 9(4):287-296.
28. Amin NU, Asad M, Chaudhry SA. An authenticated key agreement with rekeying for secured body sensor networks based on hybrid cryptosystem. Proceedings of the 9th IEEE International Conference on Networking, Sensing and Control (ICNSC). 2012 Apr, 118-121.
29. Rizk R, Alkady Y. Two-phase hybrid cryptography algorithm for wireless sensor networks. Journal of Electrical Systems and Information Technology. 2015 Dec; 2(3):296-313.
30. Anita EAM, Geetha R, Kannan E. A novel hybrid key management scheme for establishing secure communication in wireless sensor networks. Journal of Wireless Personal Communications. 2015 Jun; 82(3):1419-1433.
31. Lu H, Li J, Guizani M. Secure and efficient data transmission for cluster-based wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems. 2014 Mar; 25(3):750-761.
32. Biswas K, Muthukkumarasamy V, Sithirasenan E, Singh K. A simple lightweight encryption scheme for wireless sensor networks. Distributed Computing and Networking. 2014 Jan, 499-504.
33. Chu F, Zhang R, Ni R, Dai W. An Improved Identity Authentication Scheme for Internet of Things in Heterogeneous Networking Environments. NBIS '13Proceedings of the 2013 16th International Conference on Network-Based Information Systems. 2013 Sep, 589-593.
34. Liu Z, Wenger E, Grobschqadl J. MoTE-ECC: Energy-scalable elliptic curve cryptography for wireless sensor networks. Applied Cryptography and Network Security. 2014 Jun, 361-379.
35. Kirtiraj Bhatele, Sinhal A, Pathak M. A novel approach to the design of a new Hybrid security protocol Architecture. Proceedings of the IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT). 2012 Aug, 429-433.