American Journal of Applied Sciences 9 (6): 858-864, 2012
ISSN 1546-9239

Energy Constrained Secure Hierarchical Data Aggregation in Wireless Sensor Networks

[1]Bhoopathy, V. and [2]R.M.S. Parvathi
[1]Department of Computer Science and Engineering,
Annai Mathammal Sheela Engineering College, Tamil Nadu, India
[2]Department of Computer Science and Engineering,
Sengunthar College of Engineering, Tamil Nadu, India

Abstract: Problem statement: Wireless sensor networks, brings out variety of different challenges at energy level, integrity, authentication, communication cost. **Approach:** In the secure data aggregation techniques, reduction in the energy consumption was not elaborated in detail, since aggregator means of connection to sink was either direct or through other aggregators which need high energy level. **Results:** We suggest an Energy Constrained Secure Hierarchical Data Aggregation in Wireless Sensor Networks. At first the network was divided into clusters, each cluster begins with an aggregator and aggregator was connected to sink. Based on distance to sensor nodes and its energy level the aggregator detects the node. Separate keys were distributed to the two levels i.e., sensor node to the aggregator and aggregator to the sink. Whenever a data had to be sent from a sensor node to another node; initially the sensor node encrypts the data using a key and sends it to the aggregator. **Conclusion/Recommendations:** The digital signature algorithm that is based on the Elliptic Curve Digital Signature Algorithm is as secure and has reduced energy consumption.

Key words: Wireless Sensor Networks (WSN), Secure Hierarchical Data Aggregation (SHDA), Elliptic Curve Digital Signature Algorithm (ECDSA), Energy Efficient Secure Data Aggregation (EESDA)

INTRODUCTION

Wireless sensor networks: Wireless sensor networks consist of the latest technology that has attained notable consideration from the research community. Sensor networks consist of numerous low cost, little devices and are in nature self organizing ad hoc systems. The job of the sensor network is to monitor the physical environment, gather and transmit the information to other sink nodes. Generally, radio transmission ranges for the sensor networks are in the orders of the magnitude that is lesser that of the geographical scope of the unbroken network. Hence, the transmission of data is done from hop-by-hop to the sink in a multi-hop manner. Reducing the amount of data to be relayed thereby reduces the consumption of energy in the network (Vass and Vidacs, 2007).

Wireless sensor network consists of a huge number of tiny electromechanical sensor devices that are capable of sensing, computing and communicating. These electromechanical sensor devices can be made use for gathering sensory information, like measurement of temperature from an extensive geographical area (Kohonen, 2004).

Many features of the wireless sensor networks have given rise to challenging problems (Hartl and Li, 2004). The most important three characteristics are:

- Sensor nodes are exposed to maximum failures
- Sensor nodes which make use of the broadcast communication pattern and have severe bandwidth restraint
- Sensor nodes have inadequate amount of resources

Data aggregation: Data aggregation is considered as one of the basic dispersed data processing measures to save the energy and minimize the medium access layer contention in wireless sensor networks (Ye *et al*., 2006). It is used as an important pattern for directing in the wireless sensor networks. The fundamental idea is to combine the data from different sources, redirect it with the removal of the redundancy and thereby reducing the number of transmissions and also saves energy (Krishnamachari *et al*., 2002). The inbuilt redundancy in the raw data gathered from various sensors can be banned by the in-network data aggregation. In addition, these operations utilize raw

Corresponding Author: Bhoopathy, V., Department of CSE, Annai Mathammal Sheela Engineering College, Tamil Nadu, India

materials to obtain application specific information. To conserve the energy in the system thereby maintaining longer lifetime in the network, it is important for the network to preserve high incidence of the in-network data aggregation (Fan *et al*., 2007).

Secure data aggregation: The following are the issues that are related to the security in the data aggregation of WSN (Sang *et al*., 2006).

Data confidentiality: In particular, the fundamental security issue is the data privacy that protects the transmitted data which is sensitive from passive attacks like eavesdropping. The significance of the data confidentiality is in the hostile environment, where the wireless channel is more prone to eavesdropping. Though cryptography provides plenty of methods, such as the process related to complicated encryption and decryption, like modular multiplication of large numbers in public key based on cryptosystems, utilizes the sensor's power speedily.

Data integrity: It avoids the modification of the last aggregation value by the negotiating source nodes or aggregator nodes. Sensor nodes can be without difficulty compromised because of the lack of the expensive tampering-resistant hardware. The otherwise hardware that has been used may not be reliable at times. A compromised message is able to modify, forge and discard the messages.

Generally, in wireless sensor networks for secure data aggregation, two methods can be used. They are hop by hop encrypted data aggregation and end to end encrypted data aggregation (Sang *et al*., 2006).

Hop-by-Hop encrypted data aggregation: In this technique, the encryption of the data is done by the sensing nodes and decryption by the aggregator nodes. The aggregator nodes aggregate the data and again encrypt the aggregation result. At the end, the sink node that obtains the last encrypted aggregation result decrypts it.

End to end encrypted data aggregation: In this technique, the aggregator nodes in between does not contain any decryption keys and can only perform aggregation on the encrypted data.

Related work: Sang *et al*. (2006) have classified in concern with the security issues, data confidentiality and integrity in data aggregation into hop-by-hop encrypted data aggregation and end-to-end encrypted data aggregation. They have also proposed two general frameworks for these two correspondingly. The framework for end-to-end encrypted data aggregation has high computation cost on the sensor nodes, but attains stronger security, when compared to the framework for hop-by-hop encrypted data aggregation.

Prakash *et al*. (2009) have offered privacy-preserving data aggregation method for additive aggregation functions. The objective of their work is to connect the gap between collaborative data collection by wireless sensor networks and data privacy. They have presented simulation results of their methods and compared their performance to a typical data aggregation scheme TAG, in which there is no data privacy protection is offered. Results show the efficacy and efficiency of their methods. But, because of the algebraic properties of the polynomials, the communication overhead increases and becomes more complex.

AbuHmed and Nyang (2009) have presented a vibrant and protected scheme for data aggregation in WSN. Their proposal scheme consists of level-based key derivation, data aggregation and a new node joins phases. In addition, they have also done a security analysis for an associated Level-based Key Management (LBKM) scheme proposed by Kim *et al*. Their analysis shows that LBKM is insecure for one node compromising and nearby nodes misbehavior. To this end, they proposed various level-based key management schemes for protected data aggregation. Their scheme is protected and more efficient than LBKM scheme in concern with communication overhead and security. However, the proposed work is work only in the tree based structure. Moreover, the overhead is larger in the case of the threshold cryptography.

He *et al*. (2007) have offered two privacy-preserving data aggregation schemes for additional aggregation functions. Cluster-based Private Data Aggregation (CPDA) is their first scheme that leverages the clustering protocol and algebraic properties of polynomials. Slice-Mix-Agg Rega Te (SMART) is their second scheme that builds on slicing techniques and the associative property of addition. The objective of their work is to connect the gap between collaborative data collection by wireless sensor networks and data privacy. They evaluated the two schemes by privacy-preservation efficacy, communication overhead and data aggregation accuracy. Their Simulation outcome shows the efficacy and efficiency of our schemes. But the bandwidth use is increased in the case of their proposed SMART technique.

Huang and Shieh (2007) have proposed a Secure Encrypted-Data Aggregation (SEA) scheme in Mobile Wireless Sensor Networks (MWSN) environment. Their design for data aggregation removes redundant sensor readings which does not uses encryption and maintains data privacy and privacy during transmission. When compared to conventional schemes, their

proposed scheme provides security and privacy and duplicate instances of original readings will be aggregated into a single packet; thereby, more energy can be saved. But integrity is not brought into discussion in their proposed SEA scheme.

Chan *et al*. (2006) Secure hierarchical in-network data aggregation is guaranteed to identify any manipulation of the aggregate by the adversary beyond what is achievable through direct injection of data values at compromised nodes. In other words, the adversary can never gain any advantage from misrepresenting intermediate aggregation computations. The system incurs only O (Δlog2 n) node congestion, supports arbitrary tree-based aggregator topologies and retains its resistance against aggregation manipulation in the presence of arbitrary numbers of malicious nodes. The main algorithm is based on performing the SUM aggregation securely by first forcing the adversary to commit to its choice of intermediate aggregation results.

Problem identification: In study Bhoopathy and Parvathi (2011), we had proposed an Energy Efficient Secure Data Aggregation Protocol for wireless sensor networks. In this protocol, we incorporate the authentication and security to maintain the efficiency of the data aggregation. Whenever a sensor node wants to send data to another node; first the sensor node encrypts the data using a key and sends it to the aggregator. For integrity of the data packet, a MAC based authentication code is used. The security problem of WSN such as aggregator compromise is not taken into consideration. This aggregator compromise is harmful for network communication in network data aggregation.

MATERIALS AND METHODS

We propose an energy constrained secure hierarchical data aggregation in wireless sensor networks

Proposed work:

System overview: Initially we describe the details for the algorithm that will be executed at the sensors. Appropriate elliptic curve parameters, the base stations' public key and a network wide random integer will be pre-loaded for each sensor. The integer is made use to generate a new k at set intervals. This assures that the signatures are additive and are secure against attacks. At the beginning of each round, each sensor selects a private key and calculates the appropriate public key. Selecting a private key is straightforward and needs the sensor to select an integer in the field of the elliptic curve. The public key is produced by multiplying the base point T with the private key; as a result another point is produced on the curve. A new public/private key pair is required in each round of processing since it would take only two signatures for a malicious node thereby will determine another node's private key. If a sensor signs the same reading with the same key, then another sensor would be able to decide the private key. In most sensor applications, it's likely that the same message would be generated several times. Each sensor calculates R, which is the base point T multiplied by the current random integer k. In addition, each sensor will calculate the multiplicative inverse of k mod p. Now each sensor can produce its unique signature si. Once the signature has been generated, the sensor proceeds to homomorphically encrypt its reading xi. Initially the sensor maps its reading onto the elliptic curve. Once the mapping is done, the reading is encrypted using the ECIES algorithm (Liu and Ning, 2008).

When the sensor receives messages from other nodes for forwarding, it unites them based on the algorithm. The signature scheme is designed in such way that all signatures can be united via simple arithmetic. This will make the amount of work necessary from a parent very small and thus well suited for wireless sensor networks.

Algorithm for Sensor:

Requirement: Elliptic Curve Parameters E = (q, Fr, a, b, T, p, h), sensor reading mi, private key Pi, sink public key Pu, a network wide random integer k

Step 1 = The sensor node calculates Pi * T = (x, y), its public key.
Step 2 = The sensor node calculates R = (r(x), r(y)) = $k_* T$.
Step 3 = The sensor node calculates k^{-1} mod p.
Step 4 = The sensor node calculates si = k^{-1} (mi + Pi $_*$ r(x)) mod p.
Step 5 = Each sensor node's signature for the message mi is si.
Step 6 = Each sensor node maps its reading mi onto the elliptic curve E.
Step 7 = Each sensor node generates cipher-text mi = enc (mi)
Step 8 = If Sensor node is a parent then
Step 9 = The sensor node combines the signatures into s =∑si
Step 10 = The sensor node combines all cipher-texts into one cipher-text ∑mi
Step 11 = End if

Algorithm for base station:

Requirement: Elliptic Curve Parameters E = (q, Fr, a, b, T, p , h), sum of encrypted sensor readings m =$\sum m_i$, sum of the signatures s ==$\sum s_i$, base station private key q_i, sum of public keys Z, a network wide random integer k

Step 1 = Decrypt cipher-text $\sum m_i$ = =$\sum m_i$
Step 2 = Map reading m from the elliptic curve D into plaintext.
Step 3 = Calculate R = (r(x), r(y)) = k * T.
Step 4 = Calculate w = s^{-1} mod p.
Step 5 = Calculate u1 = mw mod p.
Step 6 = Calculate u2 = r(x) w mod p.
Step 7 = Calculate X = $u_1T + u_2Z$.
Step 8 = Calculate v = X(x) mod p.
Step 9 = If v == r then
Step 10 = The signature verified
Step 11 = End if

The algorithm explained securely computes the SUM of the readings in a wireless sensor network. The base station needs a count of the number of points included in the SUM, to securely compute the AVERAGE in a wireless sensor network. By knowing the count of sensors contributed to the aggregate, the AVERAGE can be calculated.

RESULTS AND DISCUSSION

Simulation setup: The performance of our ECSHDA protocol is estimated through Network Simulator Version-2 Ns-2 simulation (Fig. 1-11). A random network deployed in an area of 351×351 m is considered. Initially 30 sensor nodes are placed in square grid area by placing each sensor in a 50×50 grid cell. 4 phenomenon nodes which move across the grid (speed 5m sec^{1}) are deployed to trigger the events. 4 aggregators are deployed in the grid region according to our protocol. The sink is assumed to be situated 100 meters away from the above specified area. In the simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. The Distributed Coordination Function (DCF) of IEEE 802.11 is used for wireless LANs as the MAC layer protocol. The simulated traffic is CBR with UDP source and sink. The number of sources is fixed as 4 around a phenomenon. Table 1 summarizes the simulation parameters used.

Performance metrics: The performance of an Energy Constrained Secure Hierarchical Data Aggregation (ECSHDA) protocol is compared with our previous work Energy Efficient Secured Data Aggregation (EESDA) protocol (Bhoopathy and Parvathi, 2011). The performance is evaluated mainly, according to the following metrics.

Table 1: Simulation Parameters

No. of nodes	30
Area size	351×351
Mac	802.11
Routing protocol	DSDV
Simulation time	50 sec
Traffic source	CBR
Packet size	50 bytes
Rate	50 bytes
Transmission range	150 m
No. of events	4
No. of sources	1, 2, 3 and 4
No. of attackers	1,2,3,4 and 5
Speed of events	5 m sec^{1}

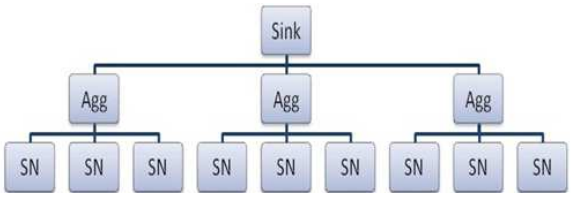

Fig. 1: System Architecture

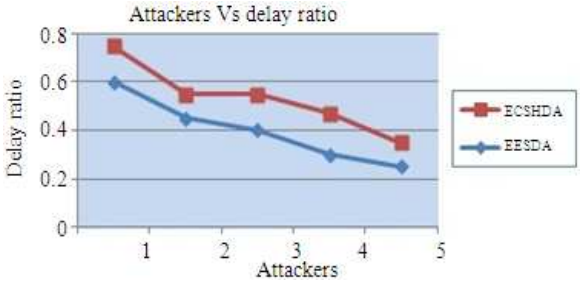

Fig. 2: When the number of nodes is increased Attackers Vs Delay gives the average end-to-end delay for both protocols. It is obvious that the average end-to-end delay of our proposed ECSHDA protocol is less than that of the existing EESDA protocol

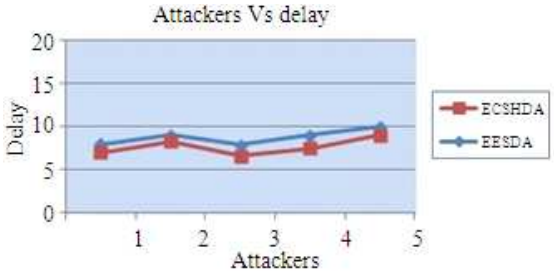

Fig. 3: Attackers Vs Delivery ratio gives the packetdelivery ratio for both protocols when the number of nodes is increased. We can observe that the packet delivery ratio of our proposed ECSHDA protocol is higher than that of the existing EESDA protocol

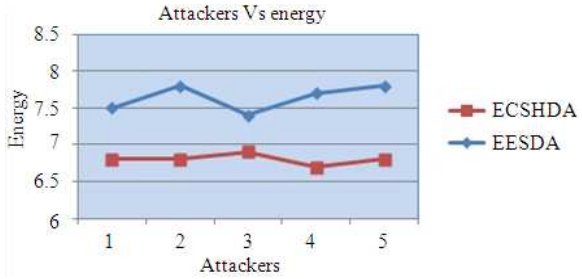

Fig. 4: Attackers Vs energy gives the enery consumption for both protocols. We can notice that the energy consumption of our proposed ECSHDA protocol is less than that of the existing EESDA protocol

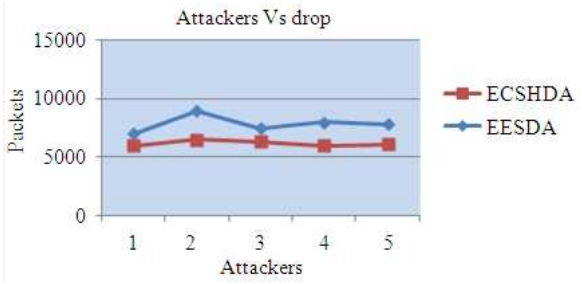

Fig. 5: Attackers Vs drop gives the Packet drop ratio for both protocols. We can make out that the Packet drop ratio of our proposed ECSHDA protocol is less than that of the existing EESDA protocol

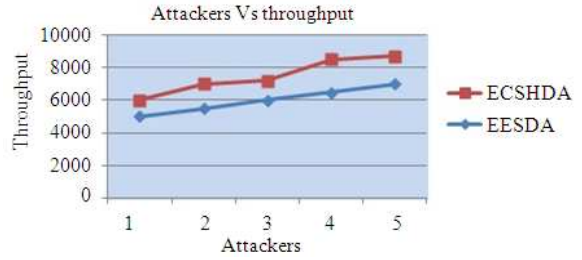

Fig. 6: Attackers Vs throughput gives thethroughput for both protocols. We can observe that the Throughput of our proposed ECSHDA protocol is higher than that of the existing EESDA protocol

The performance of ECSHDA is compared with the EESDA (He *et al*., 2007) protocol. The performance is estimated mainly, according to the following metrics.

Average end-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

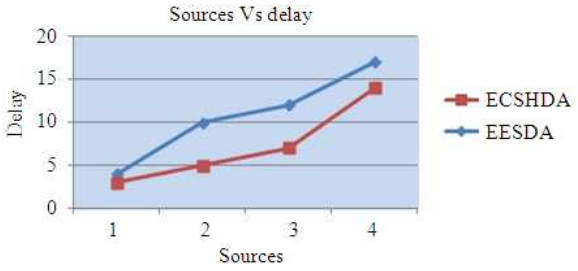

Fig. 7: Sources Vs delay gives the average end-to-end delay for both protocols when the number of sources increased.We can notice that the average end-to-end delay of our proposed ECSHDA protocol is less than that of the existing EESDA protocol

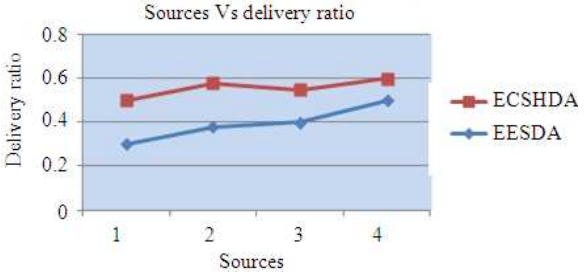

Fig. 8: Sources Vs delivery ratio gives the packet delivery ratio for both protocols We can observe that the packet delivery ratio of our proposed ECSHDA protocol is higher than that of the existing EESDA protocol

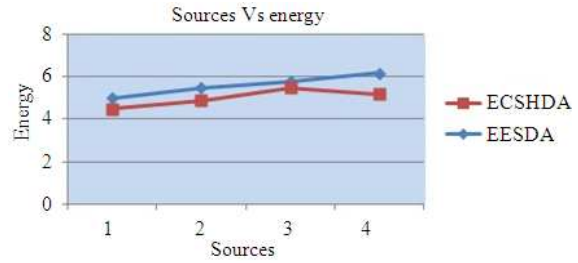

Fig. 9: Sources Vs Energy gives the enery consumption for both protocols. We can notice that the energy consumption of our proposed ECSHDA protocol is less than the existing EESDA protocol

Average packet delivery ratio: It is the ratio of the number of packets received successfully to the total number of packets transmitted.

Energy consumption: It is the average energy consumption of all nodes in sending, receiving and forward operations.

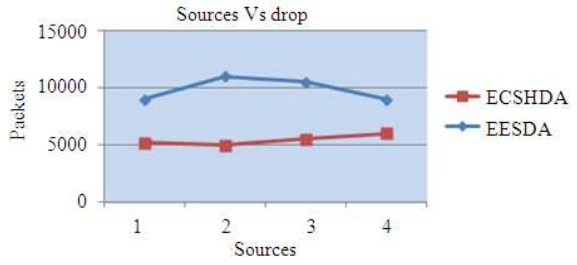

Fig. 10: Sources Vs Drop gives the Packet drop ratio for both protocols. We can notice that the Packet drop ratio of our proposed ECSHDA protocol is less than that of the existing EESDA protocol

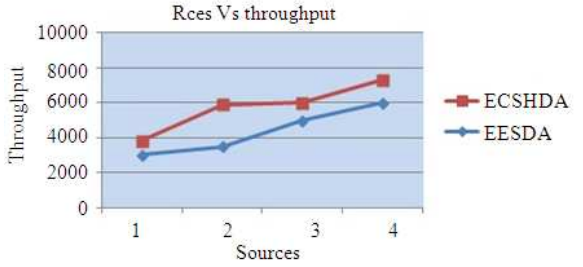

Fig. 11: Sources Vs Throughput gives the throughput for both protocols. We can observe that the Throughput of our proposed ECSHDA protocol is higher than that of the existing EESDA protocol

Average packet drop ratio: It is the ratio of the number of packets dropped to the total number of packets transmitted.

Throughput: It is the average rate of successful message delivery over a communication channel.

Based on attackers: In our initial experiment, we vary the number of attackers as 1,2,3,4 and 5

CONCLUSION

In this study, we have proposed a secure hierarchical data aggregation in wireless sensor networks that maintains energy constrained. While data aggregation, the network is separated into number of cluster and each cluster begins with an aggregator and aggregator acts as an interface between the sensor and the sink. First the encryption is completed by the sensor node using aggregator's public key and sensor's private key during the transmission of data. The decryption is done on the aggregator side using public key of sensor node and reads data. An additively digital signature algorithm dependent on ECDSA that is used to achieve integrity of the aggregate. Simulation performances show that our proposed technique has reduced energy consumption and obtained more secured.

REFERENCES

AbuHmed, T. and D. Nyang, 2009. A dynamic level-based secure data aggregation in wireless sensor network. Information Security Research Laboratory Graduate School of IT and Telecommunication InHa University.

Bhoopathy, V. and R.M.S. Parvathi, 2011. Energy efficient secure data aggregation protocol for wireless sensor networks. Eur. J. Sci. Res., 50: 48-58.

Chan, H., A. Perrig and D. Song, 2006. Secure hierarchical in-network aggregation in sensor networks. Proceedings of the 13th ACM Conference on Computer and Communications Security, Oct. 30-Nov. 03, ACM, Alexandria, VA, USA., pp: 278-287. DOI: 10.1145/1180405.1180440

Fan, K.W., S. Liu and P. Sinha, 2007. Structure-free data aggregation in sensor networks. IEEE Trans. Mobile Comput., 6: 929-942. DOI: 10.1109/TMC.2007.1011

Hartl, G. and B. Li, 2004. Loss inference in wireless sensor networks based on data aggregation. Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, Apr. 26-27, ACM, Berkeley, CA, USA., pp: 396-404. ISBN-10: 1-58113-846-6, DOI: 10.1145/984622.984680

He, W., X. Liu, H. Nguyen, K. Nahrstedt and T. Abdelzaher, 2007. PDA: Privacy-preserving data aggregation in wireless sensor networks. Proceedings of the 26th IEEE International Conference on Computer Communications, May 6-12, IEEE Xplore Press, Anchorage, AK, pp: 2045-2053. DOI: 10.1109/INFCOM.2007.237

Huang, S.I. and S. Shieh, 2007. SEA: secure encrypted-data aggregation in mobile wireless sensor networks. proceedings of the International Conference on Computational Intelligence and Security, Dec. 15-19, IEEE Xplore Press, Harbin, pp: 848-852. DOI: 10.1109/CIS.2007.207

Kohonen, J., 2004. Data gathering in sensor networks. Helsinki Institute for Information Technology, Finland.

Krishnamachari, L., D. Estrin and S. Wicker, 2002. The impact of data aggregation in wireless sensor networks. Proceedings of the 22nd International Conference on Distributed Computing Systems Workshop, (DCSW' 02), IEEE Xplore Press, pp: 457-458. ISBN-10: 0769515851, DOI: 10.1109/ICDCS.2002.1022289

Liu, A and P. Ning, 2008. Tinyecc: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks. In 7th International Conference on Information Processing Sensor Networks (IPSN' 2008), pp: 245-256.

Prakash, G.L., S.H. Manjula, K.R. Venugopal and L.M. Patnaik, 2009. Secure data aggregation using clusters in sensor networks. Int. J. Wireless Netw. Commun., 5: 93-101.

Sang, Y., H. Shen, Y. I.noguchi, Y. Tan and N. Xiong, 2006. Secure data aggregation inwireless sensor networks: A survey. Proceedings of the 7th International Conference on Parallel and Distributed Computing, Applications and Technologies, (PDCAT' 06), IEEE Xplore Press, Taipei, pp: 315-320. DOI: 10.1109/PDCAT.2006.96

Vass, D. and A. Vidacs, 2007. Distributed data agregation with geographical routing in wireless sensor networks. Proceedings of the IEEE International Conference on Pervasive Services, Jul. 15-20, IEEE Xplore Press, Istanbul, pp: 68-71. DOI: 10.1109/PERSER.2007.4283891

Ye, Z., A.A. Abouzeid and J. Ai, 2006. Optimal policies for distributed data aggregation in wireless sensor networks. Rensselaer Polytechnic Institute, USA.