IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 7, July 2016

Mask-SDA: Secure Aggregated Data Sensing Over Hetrogeneous Wireless Sensor Networks

Dr. R. Priya[1], Mr. S. Sundaramoorthi[2]

Head, Department of Computer Science, Sree Narayana Guru College, Coimbatore[1]

Assistant Professor, Dept of Computer Science &Applications, Sasurie College of Arts & Science, Vijayamangalam[2]

Abstract: A Wireless Sensor Network consists of spatially distributed sensor nodes. In a WSN, each sensor node is able to independently perform some processing and sensing tasks. Furthermore, sensor nodes communicate with each other in order to forward their sensed information to a base station. Wireless sensor networks have limited computational power and limited memory and battery power, this leads to increased complexity for application developers and often results in applications that are closely coupled with network protocols. In Data aggregation the sensor nodes can monitor the environment by collecting information from their surroundings, and work cooperatively to send the data to a base station, or sink, for analysis. Homomorphic encryptions have been applied only in Homogeneous environment not for heterogeneous environment. The existing schemes become insecure in case some sensor nodes are compromised. Existing schemes may suffer unauthorized aggregation attacks. The above problems are solved using Masked secure data aggregation scheme.

Keywords: Sensor nodes, Base station, Homomorphic encryptions, masked secure data aggregation.

NEED FOR DATA AGGREGATION IN WIRELESS SENSOR NETWORKS

With advance in technology, sensor networks composed of small and cost effective sensing devices equipped with wireless radio transceiver for environment monitoring have become feasible. The key advantage of using these small devices to monitor the environment is that it does not require infrastructure such as electric mains for power supply and wired lines for Internet connections to collect data, nor need human interaction while deploying.

These sensor nodes can monitor the environment by collecting information from their surroundings, and work cooperatively to send the data to a base station, or sink, for analysis. The main goal of data aggregation algorithms is to gather and aggregate data in an energy efficient manner so that network lifetime is enhanced. Wireless sensor networks (WSN) offer an increasingly attractive method of data gathering in distributed system architectures and dynamic access via wireless connectivity. Clustering in WSN [17]; the process of grouping the sensor nodes in a densely deployed large-scale sensor network is known as clustering. The intelligent way to combine and compress the data belonging to a single cluster is known as data aggregation in cluster based environment. There are some issues involved with the process of clustering in a wireless sensor network. First issue is, how many clusters should be formed that could optimize some performance parameter. Second could be how many nodes should be taken in to a single cluster. Third important issue is the selection procedure of cluster-head in a cluster. Another issue is that user can put some more powerful nodes, in terms of energy, in the network which can act as a cluster-head and other simple node work as cluster-member only.

Sensor networks composed of small and cost effective sensing devices equipped with wireless radio transceiver for environment monitoring have become feasible. The key advantage of using these small devices to monitor the environment is that it does not require infrastructure such as electric mains for power supply and wired lines for Internet connections to collect data, nor need human interaction while deploying. These sensor nodes can monitor the environment by collecting information from their surroundings, and work cooperatively to send the data to a base station, or sink, for analysis. The main goal of data aggregation algorithms is to gather and aggregate data in an energy efficient manner so that network lifetime is enhanced. WSN offer an increasingly attractive method of data gathering in distributed system architectures and dynamic access via wireless connectivity.

Sensor networks are collection of sensor nodes which co-operatively send sensed data to base station. As sensor nodes are battery driven, an efficient utilization of power is essential in order to use networks for long duration hence it is needed to reduce data traffic inside sensor networks, reduce amount of data that need to send to base station.

The main goal of data aggregation algorithms is to gather and aggregate data in an energy efficient manner so that network lifetime is enhanced. WSN offer an increasingly Sensor nodes need less power for processing as compared to transmitting data. It is preferable to do in network processing inside network and reduce packet size. One such approach is data aggregation which attractive method

of data gathering in distributed system architectures and dynamic access via wireless connectivity. Wireless sensor networks have limited compute.
Rational power and limited memory and battery power, this leads to increased complexity for application developers and often results in applications that are closely coupled with network protocols. In this proposed system is data aggregation framework on wireless sensor networks is presented. The framework works as a middleware for aggregating data secure measured by a number of nodes within a network.

Mask_SDA System

In WSN, data aggregation scheme that reduces a large amount of transmission is the most practical system. In earlier analysis, the homomorphic encryptions have been applied to hide and cover the communication during aggregation such that enciphered data can be aggregated algebraically without decryption. Since aggregators collect data without decryption, adversaries are not able to forge aggregated results by compromising them. However, these schemes are not satisfy multi-application environments. In WSN, the attacker can modify the data content at the time of aggregation without compromising any SN or CH. An adversary can only eavesdrop on packets in the air, so he can modify or inject the forged messages with this public information Second, these schemes become insecure in case some sensor nodes are compromised. Third, these schemes do not provide secure counting; thus, they may suffer unauthorized aggregation attacks. False data injection at the time of aggregation is one of the big issues. To overcome these problems several solutions introduced by different authors, even though the solution limits the use of WSN in heterogeneous way. Therefore, we propose a new masked ie secure data aggregation scheme, which extended from improved homomorphic encryption system known as Hidden Vector Encryption (HVE).

Secure data aggregation with false data filtering in heterogeneous network is an intricate task. To perform the same, our approach proposes a new secure aggregation scheme named as Mask_SDA, which is based on the combination of appropriate cryptographic primitives in heterogeneous clustered WSNs. The proposed system aims to develop the following for fine grained access.

- An enriched version of homomorphic algorithm, which is based on Hidden vector encryption scheme, has been used for false data injection verification and data aggregation.
- Mask_SDA overcomes the problem of existing homomorphic technique in heterogeneous environment with cost minimization.
- To reduce the total time taken for encryption, verification, decryption processes and to achieve end to end privacy, this implements MASK scheme.
- Here only the Base Station (BS) can decrypt the encrypted aggregated data by the hops. In hop by hop verification and CH based verification, the BS verifies the data, which received from member nodes in each cluster.
- To provide hop-by-hop verification, SDA use a Non-pair based identity based signature (IBS) scheme, consequently the BS and the CHs can verify the authenticity of all the transmitted encrypted data.
- To improve efficiency of multiple signature verifications, this need an effective signature scheme in which many signatures from different signers on different messages can be verified quickly.

The proposed system identifies and implements a distinct unique design for secure and continuous aggregation in wireless sensor networks. The proposed scheme applies a new scheme to protect the false data integrity and helps to authenticate the aggregated result, this also lead the energy efficient data collection over heterogeneous WSN. The advantages of the proposed system are the authenticity and verification is very fast and simple, because the scheme only needs to check a little portion of the aggregated data. This utilizes the feature of HVE and the time window. This greatly reduces the verification cost.

A. Network Model

A WSN is controlled by a base station abbreviated as BS. The BS has huge resources, sufficient memory, strong computing capability and stable power to support the cryptographic and routing requirements of the whole HWSN (Heterogeneous WSN). Moreover the BS in network, Sensor Nodes (SNs) is also deployed to sense and gather secure results for the BS in the wireless environment. SNs are limited on computation, communication capability and storage. In general, every SNs in a WSN may be divided into several clusters. Cluster-based WSN has several advantages such as efficient energy management, better scalability of MAC or routing. Each cluster has a cluster head responsible for collecting and aggregating sensing data from SNs within the same cluster. A CH then sends the aggregation results to the BS. In a heterogeneous WSN, cluster heads are selected based on different aspects. The followings are the two types of clustering in heterogeneous WSN. Usually the cluster heads act as by highest priority sensors (H-Sensors), in a heterogeneous WSN which incorporates different types of SNs with different capabilities.
This process presents the cluster-based architecture to construct the topology. Nodes cooperate to form clusters, and each cluster consists of a CH along with some Cluster Members (CMs) located within the transmission range of their CH. Before nodes can join the network, they have to obtain valid identity at the time of initialization, so that nodes can communicate with each other unrestrainedly in a WSN.

The IDs are divided into 2 categories.

1. Logical (Logical Group- LG)

Due to the nature of heterogeneous network, the proposed system uses Logical group for aggregation. It clusters the nodes based on the logical similarities, such as a secure

DOI 10.17148/IJARCCE.2016.57131

attribute based hop-by-hop aggregation is performed in each group to generate a group aggregate. The base station then identifies the suspicious groups based on the set of group aggregates.

2. Physically (Physical Group –PG)
Physical group is nothing but the similar types of sensor will be grouped together, for example all temperature detection sensors are a single group and all humidity detection sensors are another group. Based on the type and its properties, the SNs will be grouped. The following fig shows the two types of node grouping techniques.

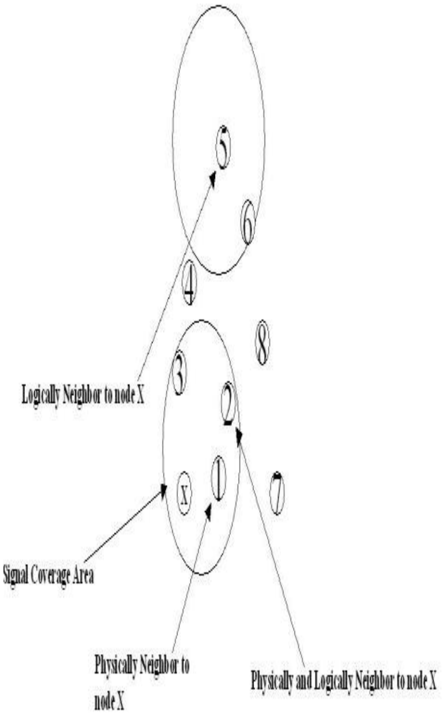

5
6
4
8
Logically Neighbor to node X
3
2
X
1
7
Signal Coverage Area
Physically Neighbor to node X
Physically and Logically Neighbor to node X

Fig 4.1: Physical and logical group example

LG is based on the identical functionality of sensor nodes, though a node can have identifications more than one group to indicate, that the node can participate in more than one environment. In the above fig 4.1 node 1 and node 5 are in Physics Group and Logical Group X node respectively, but the node 2 is included in both groups such as LG and PG. In each of LG every node may receive packets that are listed for the whole group though PG nodes are neighbors there interested node can receive these packets.

B. Attack Model
The attack model is defined based on the capacity of attackers. The abilities of the attacker have been listed below.

1. Adversaries can eavesdrop on transmission data in a WSN.
Without compromising any SN or CH. An adversary can only eavesdrop on packets, so adversary can modify or inject the fake data messages with the public information

2. Adversaries can send forged data to any entities in a WSN (e.g., SN, AG, or BS).
3. Adversaries can compromise secrets in SNs or AGs through capturing them.
The attacker can compromising SNs. After compromising a SN, an adversary can obtain secrets such as encryption/ decryption keys. Then, an adversary can obtain sensing data and packets passed through the captured SN or impersonate this compromised sensor to forge malicious data.

4. Compromising CHs.
a. After compromising a CH, an adversary can obtain the secrets and perform the following attacks. First, an adversary can decrypt the cipher text of sensing data sent by its cluster members. Second, an adversary can generate forged aggregation results.
The Mask_SDA should overcome all the above attack in the HWSN. The proposed system overcomes the above attack based issues effectively

C. Security Model:
In heterogeneous wireless sensor network, secure aggregation without decryption is a challenging task, the Mask_SDA provides an effective way for data aggregation and false data detection using HVE scheme. The proposed process performs cryptographic and signature setting at every node in the sensor network for high security. The scheme utilizes network grouping process for two purposes such as load balancing and aggregation. The following steps represent the proposed process.

```
1 begin
2    recognize node Ni…Nn
3          signature of Ni
4          aggregatedvaluefromuppernodeofNi
5   set signature Nc for N1, N2…Nn
6       if Nc already set
7           Update (Nc);
8    Else do 5
9 for every node N. collect time and aggregated details along with the signature and
       Updatedata UTo (Nc, To)
Aggregate data Ag=Ag(t) .., Ag(t+1)
10   verify the synchronization
11   if ( UTo == Nc) then
12        update
13 else
14            Trace (node det) and declare Ni= 1
15 if  (ni=1) then
17        duplicate node Cn=Ni
18 else
19    end
20 filter Ni(data det, port)
21 end
```

In the Mask_SDA scheme, the intermediated nodes perform the data verification with IBE on cipher texts received from the sensor nodes, the aggregation of the cipher texts, and verification based on signature generation on the aggregated cipher-text without decrypting the cipher-texts. The cipher-texts encrypted under the BS's public key can be decrypted by only the BS with its decryption key x. End-to-end confidentiality of the proposed scheme is reduced to the security of the underlying HVE scheme, IBE.

The Proposed encryption scheme is a concealed data aggregation scheme based on the HVE cryptosystem. It consists of four procedures: key generation (KeyGen), encryption (Enc), aggregation (Agg), and decryption (Dec).

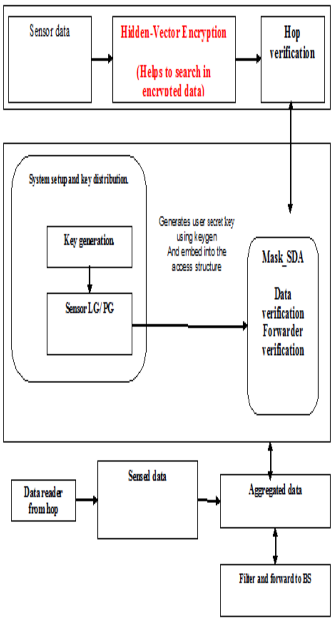

Sensor data
Hidden-Vector Encryption
(Helps to search in encrypted data)
Hop verification
System setup and key distribution.
Key generation
Sensor LG/PG
Generates user secret key using keygen And embed into the access structure
Mask_SDA
Data verification Forwarder verification
Data reader from hop
Sensed data
Aggregated data
Filter and forward to BS

Fig 4.2: Flow Diagram of Mask_SDA

This scheme consists of five procedures: key generation (KeyGen), signing (Sign), verifying (Verify), aggregation (Agg), and verifying aggregated signature with epoch. Boneh There are some important steps are involved in a HVE_IBE algorithm to solve a problem as given below:
Step 1: Assume two large prime numbers p & q.
Step 2: Compute: N = p*q Where N is the factor of two large prime number.
Step 3: Select an Encryption key (E) such that it is not a factor of (p-1)*(q-1) i.e. Ø(n)= (p-1)*(q-1) for calculating encryption exponents E, should be 1< E < Ø(n) such that gcd(E, Ø(n)=1 The main purpose of calculating gcd is that E & Ø(n) should be relative prime. Where Ø (n) is the Euler Totient Function & E is the Encryption Key.
Step 4: Select the Decryption key (D), which satisfy the Equation D*E mod (p-1)*(q-1) = 1
Step 5: For Encryption: Cipher Text= (Plain Text)E mod N CT = (PT) E mod N

The system performs the above steps in security modal, where the HVE creates with unique private key and aggregates the key at every node without decrypting them.

Epoch verification for false data filtering
After the successful data transaction, the BS verifies the data whether valid or not by selecting an agent, after the agent selection, the BS broadcasts a verification request, which includes the agent time interval, the sampling ratio and a nonce number noncev, to the WSN.

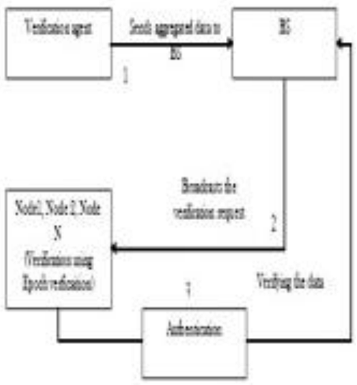

Verification agent
Sends aggregated data to BS
1
BS
Node1, Node 2, Node N (Verifications using Epoch verification)
Broadcasts the verification request
2
Verifying the data
3
Authentication

Fig 4.3: Epoch verification

Once receiving the verification request, each node decides whether to act as a sampled node. Before the sampled nodes send to the BS their sensor readings of every agent epoch, their neighboring nodes verify the correctness of test data and authenticate the sample messages. With the sensor reading samples, the BS checks the correctness of the aggregation results of each data epoch.

Using this HVE_IBE algorithm going to check whether the node aggregated correct data or not at a particular period of time. For that node is compared with all other node in the network such that: If both nodes met during that time means the message it got from that node is transferred to the nodes that are in the location mentioned in that message, for reference to other nodes and their consistency is checked. If it violates the considerations returns as attack is detected.

RESULTS AND DISCUSSION

To evaluate the performance of the proposed scheme, the execution time or aggregation delay is the main factor of performance evaluation. This defines processing delay and aggregation delay for deployed sensors. Processing delay indicates the execution time for sensors to produce cipher texts and corresponding signatures before transmission. Secure aggregation delay is also evaluated by measuring time spent on processing time on aggregating cipher texts and signature verification in the proposed schemes. The last delay, decryption delay, is not considered since the base station is considerably powerful as a workstation. Therefore, this delay is negligible and can be ignored. Another criterion is cost evaluation. Cost evaluation involves communication and computation aspects.
This proposed work was implemented using Ns2 simulation tool. The performance of this proposed work Mask_SDA using hidden vector encryption and IBE has

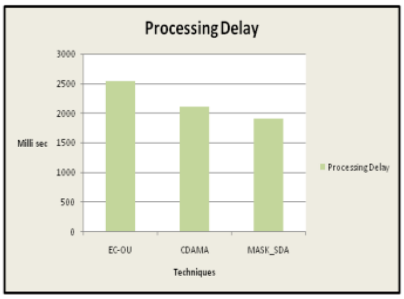
DOI 10.17148/IJARCCE.2016.57131

compared with two existing approaches CDAMA and EC-OU.

The following tables and charts shows the performance comparison of the proposed method with other existing approaches based on the six different metrics processing delay, processing energy, aggregation delay , aggregation energy, payload size and communication cost.

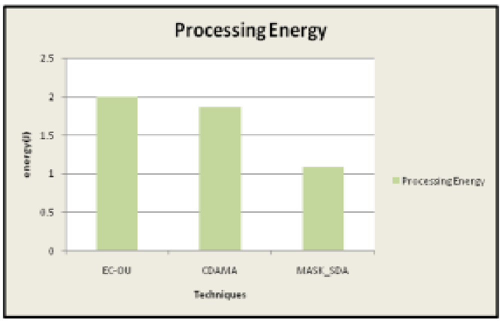
Performance comparison of proposed MASK_SDA using IBE with existing approaches based on Processing Delay

	EC-OU	CDAMA	MASK_SDA
Processing Delay	2534.09	2109.06	1902.08



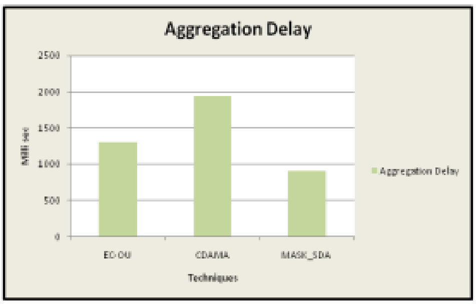
Performance comparison of proposed MASK_SDA using IBE with existing approaches based on Processing Energy

parameter	EC-OU	CDAMA	MASK_SDA
Processing Energy	2	1.86	1.08



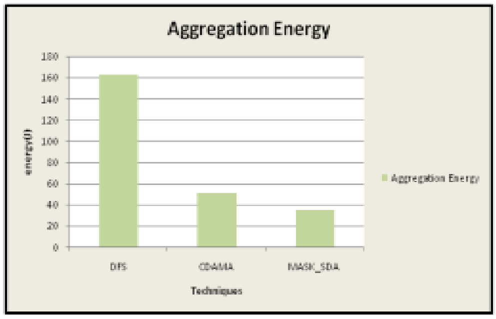
Performance comparison of proposed MASK_SDA using IBE with existing approaches based on Aggregation Delay

parameter	EC-OU	CDAMA	MASK_SDA
Aggregation Delay	1300.09	1932.06	902.08

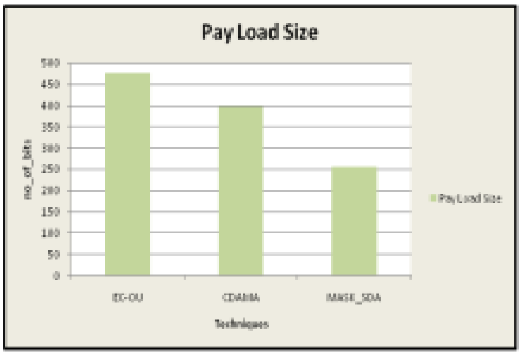


Performance comparison of proposed MASK_SDA using IBE with existing approaches based on Aggregation Energy

parameter	DFS	CDAMA	MASK_SDA
Aggregation Energy	162.5	50.9	34.9



Performance comparison of proposed MASK_SDA using IBE with existing approaches based on Pay Load Size



CONCLUSION

WIRELESS sensor networks (WSN) have been widely deployed in many applications such as health care, environmental monitoring and military field surveillance etc. A huge number of security issues threaten the current WSN, so this thesis has proposed a new secure data aggregation schemes for heterogeneous WSNs named as Mask_SDA. A special feature of the proposed work is, this can able to aggregate the data even if it is encrypted, in usual the heterogeneous network doesn't allow this type of process, so our current proposal includes an improved homomorphic algorithm such as hidden vector based identity encryption. This allows the heterogeneity node to aggregate their encrypted data over the network. With the help of epoch scheme, the system can able to filter false data from the aggregation process. This avoids the data misuse issues.

Even though signatures bring additional costs, the proposed schemes are still affordable for WSNs after evaluation, because it provides data search option in encrypted content. This has successfully implemented in NS2 tool with 50 nodes. The experiments and results shows that, the proposed work is efficient than existing CDAMA.

REFERENCES

[1] Chong, C.-Y.& Kumar, S. P. (2003). Sensor networks: Evolution, opportunities, and challenges, Proceedings of the IEEE **91**(8): 1247–1256

[2] Rashid, R. & Robertson, G. (1981). Accent: A communication oriented network operating system kernel, Proc. of the 8th Symposium on Operating System Principles, pp. 64–75.

[3] Myers, C., Oppenheim, A., Davis, R. & Dove, W. (1984). Knowledge-based speech analysis and enhancement, Proc. of the International Conference on Acoustics, Speech and Signal Processing.

[4] Kumar, S. & Shepherd, D. (2001). Sensit: Sensor information technology for the warfighter, Proc. of the 4th International Conference on Information Fusion (FUSION'01), pp. 3–9 (TuC1).

[5] ZigBee Alliance (n.d.). http://www.zigbee.org.

[6] 21 Ideas for the 21st Century (1999). BusinessWeek pp. 78–167.

[7] Ni, L.M. (2008). China's national research project onwireless sensor networks, Proc. of the 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'08), p. 19.

[8] Crossbow Technology (n.d.), http://www.xbow.com.

[9] Dust Networks, Inc. (n.d.). http://www.dustnetworks.com.

[10] Hill, J. L. (2003). System Architecture for Wireless Sensor Networks, PhD thesis, Doctor of Philosophy in Computer Science, University of California at Berkeley, USA.

[11] Sudevalayam, S. & Kulkarni, P. (2008). Energy Harvesting Sensor Nodes: Survey and Implications, Technical Report TR-CSE-2008-19, Department of Computer Science and Engineering, Indian Institute of Technology Bombay.

[12] Pister, K. S. J. (2000). Military applications of sensor networks, of Institute for Defense Analyses Paper P-3531, Defense Science Study Group. Proceedings of the Distributed Sensor Nets Workshop (1978). Pittsburgh, USA. Department of Computer Science, Carnegie Mellon University.

[13] Steere, D., Baptista, A., McNamee, D., Pu, C. & Walpole, J. (2000). Research challenges in environmental observation and forecasting systems, Proc. of 6th International Conference on Mobile Computing and Networking (MOBICOMM'00), pp. 292–299.

[14] Streetline, Inc. (n.d.). http://www.streetlinenetworks.com.

[15] Rohrback Cosasco Systems (n.d.). http://www.cosasco.com.

[16] Connolly, M. & O'Reilly, F. (2005). Sensor networks and the food industry, Proc. of Workshop on Real-WorldWireless Sensor Networks (REALWSN'05).

[17] Li, Qinghua, Guohong Cao, and Thomas La Porta. "Efficient and privacy-aware data aggregation in mobile sensing." Dependable and Secure Computing, IEEE Transactions on 11.2 (2014): 115-129.

[18] K. Dasgupta, K. Kalpakis, and P. Namjoshi, "An Efficient Clustering-based Heuristic for Data Gathering and Aggregation in Sensor Networks", IEEE 2003.

[19] 7. E. Fasolo, M. Rossi, J. Widmer, and M. Zorzi, "InNetwork Aggregation Techniques for Wireless Sensor Networks: A Survey", IEEE Wireless communication 2007.

[20] Przydatek, Bartosz, Dawn Song, and Adrian Perrig. "SIA: Secure information aggregation in sensor networks." Proceedings of the 1st international conference on Embedded networked sensor systems. ACM, 2003.

[21] Atallah, Mikhail J., et al. "Dynamic and efficient key management for access hierarchies." ACM Transactions on Information and System Security (TISSEC)12.3 (2009): 18.

[22] Cam, H; Ozdemir, S Nair, P Muthuavinashiappan, D (October 2003). "ESPDA: Energy-efficient and Secure Pattern-based Data Aggregation for wireless sensor networks". Sensors 2: 732–736.

[23] Hu, Lingxuan; David Evans (January 2003). "Secure aggregation for wireless networks". Workshop on Security and Assurance in Ad hoc Networks.

[24] Atallah, Mikhail J., et al. "Dynamic and efficient key management for access hierarchies." ACM Transactions on Information and System Security (TISSEC)12.3 (2009): 18.

[25] Kumar, Vimal; Sanjay K. Madria (August 2012). "Secure Hierarchical Data Aggregation in Wireless Sensor Networks: Performance Evaluation and Analysis". MDM 12.

[26] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Next century challenges: Scalable coordination in sensor networks," in Proceedings of ACM Mobicom, Seattle, Washington, USA, August 1999, pp. 263–270, ACM.

[27] C. Intanagonwiwat, D. Estrin, R. Govindan, and J. Heidemann, "Impact of network density on data aggregation in wireless sensor networks," in ICDCS, 2002, pp. 457–458.

[28] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," in MOBICOM, 2000, pp. 56–67

[29] David Wagner, "Resilient aggregation in sensor networks," in Proceedings of ACM Workshop SASN '04, 2004

[30] L. Hu and David Evans, "Secure aggregation for wireless networks," in Workshop on Security and Assurance in Ad hoc Networks, January 2003. . Du, J. Deng, Y. S. Han, and P. K. Varshney, "A witness-based approach for data fusion assurance in wireless sensor networks," in Proc. of IEEE GLOBECOM '03, December 2003.

[31] B. Przydatek, D. Song, and A. Perrig, "SIA: secure information aggregation in sensor networks," in SenSys '03: Proceedings of the 1st international conference on Embedded networked sensor systems, 2003, pp. 255–265.

[32] Fan Ye, Haiyun Luo, Songwu Lu, and Lixia Zhang, "Statistical en-route filtering of injected false data in sensor networks," in Proceedings of IEEE Infocom'04, 2004.

[33] W. Zhang and G. Cao, "Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration-Based Approach," IEEE INFOCOM, March 2005.

[34] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks," in Proceedings of IEEE Symp. on Security and Privacy, 2004, pp. 259–271.

[35] S. Ozdemir, "Concealed Data Aggregation in Heterogeneous Sensor Networks Using Privacy Homomorphism," Proc. IEEE Int'l Conf. Pervasive Services, pp. 165-168, July 2007

[36] H. Chan, A. Perrig, and D. Song, "Secure Hierarchical In-Network Aggregation in Sensor Networks," Proc. ACM 13th Conf. Computer and Comm. Security, pp. 278-287, 2006.

[37] Y. Yang, X. Wang, S. Zhu, and G. Cao, "SDAP: A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks," ACM Trans. Information and System Security (TISSEC), vol. 11, no. 4,pp. 1-43, 2008.

[38] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient Aggregation of Encrypted Data in Wireless Sensor Networks," Proc. Second Ann. Int'l Conf. Mobile and Ubiquitous Systems, pp. 109-117, July 2005.

[39] S. Roy, S. Setia, and S. Jajodia, "Attack-Resilient Hierarchical Data Aggregation in Sensor Networks," Proc. ACM Fourth Workshop Security of Ad Hoc and Sensor Networks, pp. 71-82, 2006.

[40] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660-670, Oct. 2002.

[41] M. Demirbas, A. Arora, V. Mittal, and V. Kulathumani, "A Fault-Local Self-Stabilizing Clustering Service for Wireless Ad Hoc Networks," IEEE Trans. Parallel Distributed Systems, vol. 17, no. 9, pp. 912-922, Sept. 2006.

[42] S. Basagni, M. Mastrogiovanni, A. Panconesi, and C. Petrioli, "Localized Protocols for Ad Hoc Clustering and Backbone Formation: A Performance Comparison," IEEE Trans. Parallel Distributed Systems, vol. 17, no. 4, pp. 292-306, Apr. 2006.

[43] H. Sanli, S. Ozdemir, and H. Cam, "SRDA: Secure Reference-Based Data Aggregation Protocol for Wireless Sensor Networks," Proc. IEEE 60th Int'l Conf. Vehicular Technology (VTC '04-Fall), vol. 7, pp. 4650-4654, Sept. 2004.

[44] Lin, Yue-Hsun, Shih-Ying Chang, and Hung-Min Sun. "CDAMA: concealed data aggregation scheme for multiple applications in wireless sensor networks."Knowledge and Data Engineering, IEEE Transactions on 25.7 (2013): 1471-1483.

[45] P. Paillier. Trapdooring Discrete Logarithms on Elliptic Curves over Rings. ASIACRYPT, pages 573–584, 2000

DOI 10.17148/IJARCCE.2016.57131