International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Survey on Several Secure Data Aggregation Schemes in WSN

Youssef Emhemmad Mohammad Youssef* **and Raghav Yadav**

Department of Computer Sciences & IT, Sam Higginbotom Institute of Agriculture, Technology & Science, Allahabad, India

Accepted 01 July 2016, Available online 11 July 2016, **Vol.6, No.4 (Aug 2016)**

Abstract

Nowadays, wireless sensor network (WSN) are used on many fields such as health monitoring, environment monitoring and target tracking, wireless sensor network (WSN), it's nothing but set of great numbers of nodes deployed in specific zone, those nodes communicating with each other's, consequent great energy consumption because of that, the lifetime of network it will be very short. Data Aggregation (DA) one of many techniques which can help to reduce the energy consumption in (WSN), and prolong the lifetime of the network, but (DA) has many challenges, one of them is the security issues, several techniques have proposed for secure data aggregation in (WSNs). The main target of this paper to introduce to different data aggregation techniques, and then discuss Secure Data Aggregation (SDA) approaches and attacks, and then to survey presented schemes for (SDA) in (WSNs), finally a comparison between schemes in some parameters.

Keywords: *Wireless Sensor Network, Data Aggregation, Secure Data Aggregation, Base Station, Cluster Head.*

1. Introduction

1.1 Wireless Sensor Network

A wireless sensor network is an ad-hoc network. It's a collection of small wireless nodes called sensor nodes, deployed in environmental or physical condition. And it measured physical parameters such as temperature, pressure, sound, and humidity. These sensor nodes deployed in a large zone and collaborate with each other to form sensor network capable of reporting to data aggregation sink (Base Station) (BS). Wireless sensor network has several applications. If talked about, energy, memory, limited communication capabilities and computation, can say that wireless sensor network is a resource constraint. All sensor nodes in the wireless sensor network are interact with each other or by intermediate sensor nodes (Kiran Maraiya *et al* 2011) as showing in figure 1.

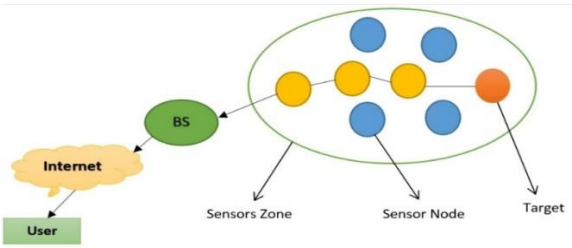

Figure 1: Architecture of the Sensor network

Sensor networks have certain limitations represented in limited of memory resources, limited bandwidth and transmission power and vulnerability of nodes to physical capture (S. Siva Ranjani *et al,* 2014).

1.2 Security Issues in WSN

The sensor networks can also work in an Ad Hoc way the security targets cover both those of the traditional networks and goals suited to the unique constraints of sensor networks. The security targets are classified as primary and secondary. The primary targets are known as standard security targets such as Integrity, Confidentiality, Availability (CIAA), and Authentication. The secondary targets are Secure Localization, Time Synchronization, Self-Organization, and Data Freshness (S. Archana *et al,* 2015).

1.3 Attacks in WSN

The WSNs are at risk to security attacks due to the broadcast nature of the transmission medium. Moreover, WSNs have extra vulnerability due to nodes are often placed in a hostile or dangerous zone where they are not physically protected. Essentially attacks are classifying as active attacks and passive attacks (S. Archana *et al,* 2015). Attacks on WSNs can be classified as showing in figure 2 (Dr. G. Padmavathi *et al,* 2009).

*Corresponding author **Youssef Emhemmad Mohammad Youssef; Dr. Raghav Yadav** is working as Assistant Professor

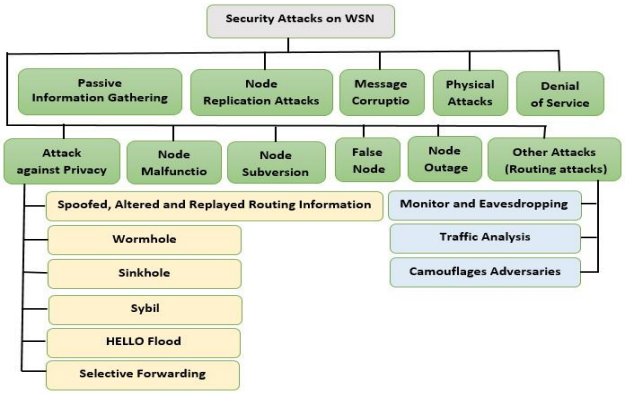

Figure 2: Classification of Security Attacks on WSN

2. Data Aggregation in WSN

Data aggregation (DA) is the best approach for energy conservation in Wireless Sensor Networks (WSN), due to the open deployment, sensors are prone for security threats (S. Siva Ranjani *et al,* 2014). In the wireless sensor network(WSN) have the hard mission, it prolongs the lifetime of the network, so with the help of data aggregation the lifetime of the network will be increased (Kiran Maraiya *et al,* 2011). Data aggregation techniques can efficiently help to cut the consumption of energy by disposing of unnecessary data traveling back to the sink, data aggregation is the process of one or several sensors then aggregation the detection result from another sensor. Data aggregation normally includes the integration of data from many sensor nodes and the aggregator node transmits the aggregated data to the (BS) (Priyanka B. Gaikwad *et al,* 2015). The aggregated data must be processed by a sensor to reduce transmission as showing in figure 3. Without data aggregation mode, in this case, the data transmits immediately without processing which leads to an increase in energy consumption as well as the lifetime of the network will be decreased because the combine and summarize the data packets of several nodes it will not happen so that amount of data transmission is increased. Showing in figure 4.

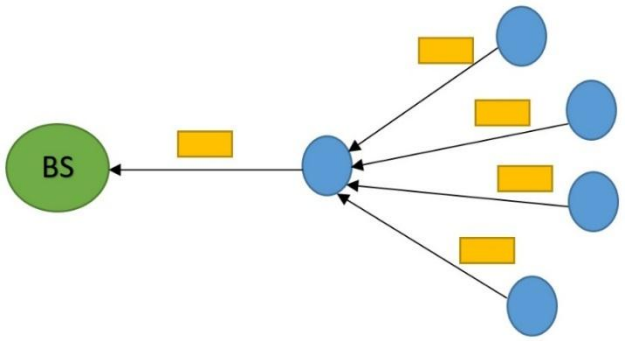

Figure 3: With DA model

Considering the advantages, and the information obtained by the entire network it's accurate and powerful, can be improved using data aggregation process. The data collected from the sensor nodes detect repeated data and then data fusion (Hevin Rajesh Dhasian *et al,* 2013). On the other hand, the aggregator node or the cluster-head may be attacked by a malicious attacker. When the cluster-head is compromised, the aggregated data which sent to (BS) it will be not guaranteed.

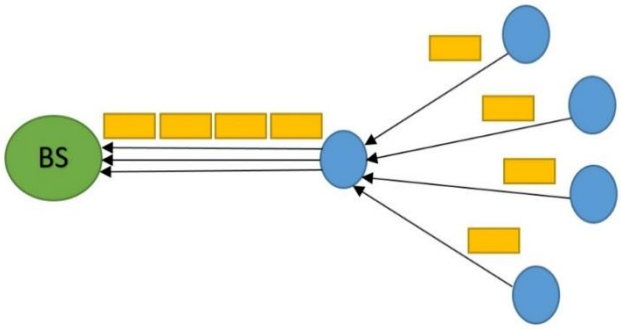

Figure 4: Without DA model

2.2 Types of Attacks on Data Aggregation in WSN

There are many types of attacks on data aggregation in WSN, in the table 1 some of them (Priyanka B. Gaikwad *et al,* 2015; Jyoti Rajput *et al,* 2014)

Table 1: Some of Attacks on DA in WSN

No.	Attack Type	Reason of Attack	Resolved
1	Replay Attack	Transmitting same data without data freshness	Using time stamp
2	Denial of service attack	Interference with radio frequency	Using MAC
3	Data Integrity Attack	Inserting false data	Using digital signature and MAC
4	Sybil attack	Making multiple identities	Using authentication schemes
5	False packet, Malleability attack	Due to injection of malicious nodes	Using HMAC
6	Sinkhole Attack	Attracting traffic to the specific danger node	Using proper routing and localization information
7	Energy Drain attack	Due to energy depletion	Making use of several energy harvesting techniques as: solar power
8	Sniffing Attack	due to capturing data by using malicious nodes	using protocols with confidentiality of data
9	Physical Attack	Due to lack security of symmetric key approach	Use of Asymmetric public key approach

2.3 Demo of Data Aggregation Techniques in (WSN)

(DA) may be a method of aggregating the sensing element knowledge victimization aggregation approaches. The overall knowledge aggregation rule works as shown in figure 4. Generally, data aggregation algorithm collected the data from sensor nodes by

using some aggregation algorithms like LEACH (Low Energy Adaptive Bunch Hierarchy), TAG (Tiny Aggregation), centralized approach etc., and then aggregated data after that transfer the data to the sink node by choosing the efficient path. The fundamental design of (DA) technique (Ameya S. Bhatlavande *et al,* 2015) as showing in Figure 5.

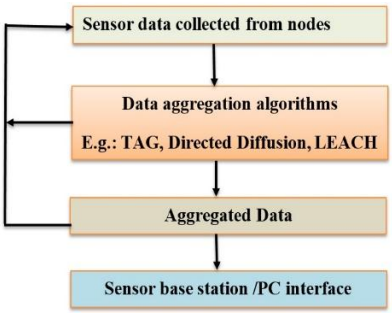

Figure 5: Architecture of DA Technique

2.3 DA Approaches

There are many approaches of DA are presented some are as follows:

- **Centralized Approach**

As showing in figure 6, only one sensor node plays in this approach a role of aggregator node and all remaining sensor nodes are connected to that aggregator node. All remaining sensor nodes sensing the data and transmit to the aggregator node, which is called centralized node. There are a lot of loads on that aggregator node, so there is a need of more energy and security on that aggregator node because all data is on the centralized aggregator node (Jyoti Rajput *et al,* 2014).

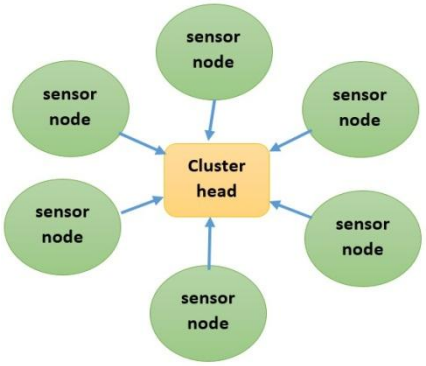

Figure 6: Centralized approach for DA in WSN

- **Decentralize approach**

All sensor nodes play aggregator function to the sensed data. Here single centralized aggregator node is not available, but all nodes have the same priority to aggregate the sensed data. Also, all sensor nodes are connected to their neighbor node. This methodology has the benefit of more scalability, dynamic change node failure in the (WSNs) (Jyoti Rajput *et al,* 2014) as showing in figure 7.

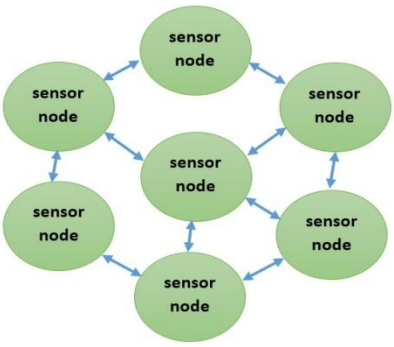

Figure 7: Decentralized approach for DA in WSN

- **Cluster-Based approach**

Here as showing in figure 8, the network is divided into several clusters. Each cluster has a Cluster-Head (CH) which be chosen from among members of the cluster, cluster heads do the role of the aggregator which aggregate data received from cluster members locally and then transmit the result to sink (BS) (Jyoti Rajput *et al,* 2014).

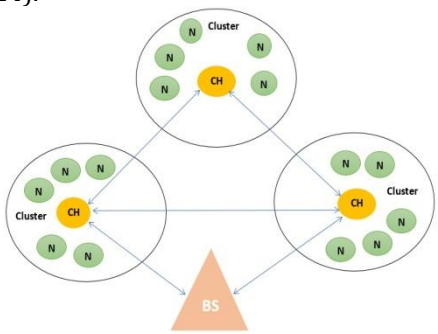

Figure 8: Cluster based approach for DA in WSN1

- **Tree-Based Approach**

As Figure 9, in this approach perform aggregation by constructing an aggregation tree, which may be a minimum spanning tree, rooted at sink and source nodes are considered leaves. Each node has a parent node to send its data. The flow of data starts from leaves nodes up to the sink (BS) and therein the aggregation done by parent nodes (Jyoti Rajput *et al,* 2014).

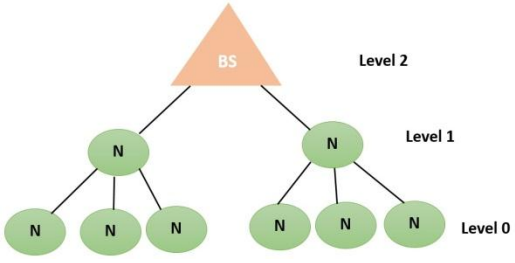

Figure 9: Tree based approach for DA in WSN

3. Classification of Existing Secure DA Schemes

Classifies the secure schemes into two models based on a number of aggregators (Priyanka B. Gaikwad *et al* 2015; Kiran Maraiya *et al* 2011):

- Single Aggregator Scheme.
- Multiple Aggregator Scheme.

Figure 10 shows some of SDA Schemes.

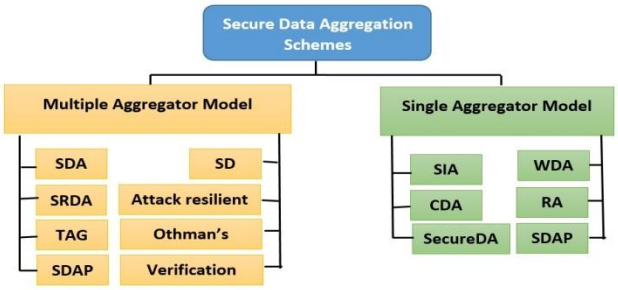

Figure 10: Classification of Existing Secure DA Schemes

4. Several of Existing Secure DA Schemes

There are several schemes that have been proposed, here some of them as following (Vasudha Khillan *et al,* 2015):

Secure Information Aggregation (SIA) (B. Przydatek *et al,* 2003) proposed framework provides resistance against a special type of attack called stealthy attack where the attacker's target is to make the user accept false aggregation results, which are much different from true results determined by the measured values, while not being detected by the user.

Secure Data Aggregation (SDA) (L. Hu *et al,* 2003) was proposed in the year 2003 also who studied the problem of data aggregation once one node is compromised. This protocol goal at providing the lightweight security mechanism to effectively detect node misbehavior (dropping, modifying or forging messages, transmitting false aggregate value).

Energy-Efficient and Secure Pattern-based Data Aggregation Protocol (ESPDA) (H. Cam *et al,* 2006) proposed to give energy-efficient DA together with secure data communication in (WSNs). It is a cluster-based data aggregation protocol. ESPDA also provides security because it aggregates data by pattern codes, so cluster-heads need not to know the contents of the transmitted data. Then, the sensor data is transmitted to base station in encrypted form without decrypted anywhere in the transmission path. ESPDA employs a Non-blocking Orthogonal Variable Spreading Factor (NOVSF) code hopping technique.

Secure Reference-Based Data Aggregation Protocol (SRDA) (H. Ozgur Sanli *et al,* 2004) SRDA that sends the differential data i.e. difference between the sensed data and the reference value instead of the raw sensed data. The reference value is taken as the average value of earlier sensor readings. Each sensor node first senses the data from the environment, then computes the differential data, encrypts it, and send it to the cluster-head. The SRDA uses a higher security margin at higher level cluster-heads compared to low-level cluster-heads. Thus, SRDA incorporates both data aggregation and security concepts together in the cluster-based wireless sensor network. SRDA provides data confidentiality, data freshness, and authentication.

Secure Data Aggregation and Verification Protocol (SecureDAV) (Dr. G. Padmavathi *et al,* 2009) that proposed to improve the data integrity vulnerability in SDA by signing the aggregated data. SecureDAV is a cluster-based data aggregation protocol. An elliptic curve cryptosystems (ECC) are used for establishing cluster keys in sensor networks using verifiable secret sharing.

Secure Hop-by-Hop Data Aggregation Protocol(SDAP) (Y. Yang *et al,* 2008) proposed the protocol which can tolerate more than one compromised node. The design of SDAP is based on two principles: divide-and-conquer and commit-and-attest. This general purpose data aggregation protocol has three steps. The first step is tree construction and query dissemination, where an aggregation tree is constructed and thereby all nodes identify their parents, after which the base station disseminates the aggregation query message through the tree. The second step is probabilistic grouping and data aggregation, in which SDAP uses the divide-and-conquer principle to divide the network tree into multiple logical subtrees based on a probabilistic grouping technique which depends on group leader selection.

The author in (Madden Samuel *et al,* 2002) discusses a tree topology used in TAG, to order to avoid double-counting sensor readings. TAG operates as follows: users insert aggregation queries from a storage-rich and powered base station. Operators that implement the query are distributed by piggybacking on the existing ad hoc networking protocol into the network. Sensor nodes route the data at the base station in the routing tree. Based on an aggregation function and value-based partitioning specified in the query, the data is aggregated.

The algorithm in (W. Du *et al,* 2003) considers a witness based data aggregation (WDA), for the single aggregator scheme to assure the validation of the data that is being sent from an aggregator node to the queries (base station). So as to prove the validation, the aggregator node needs to give proofs from many of the witness nodes. A witness node is the one who performs data aggregation but does not forward the result to the base station. The message authentication code (MAC) of the result is computed by each witness node. Then the witness node sends it to the aggregator node that forwards the proofs to the base station. Integrity property is offered by the WDA to the data aggregation security and this is needed to send many copies that are similar to the original aggregated value, to

aggregator point. Thus, these reports along with aggregated value to the base station are forwarded by the aggregator point.

The algorithm in (Ben Othman S *et al,* 2013) provides integrity and confidentiality in a novel way preserving aggregation in wireless sensor network. This algorithm uses Message Authentication Code (MAC) and homomorphic encryption (Elliptic curve ElGamal) to achieve integrity, authenticity, and confidentiality of the data. The simulation results show that the communication and computation overhead is reduced.

The author in (S. Roy *et al,* 2006) proposed the attack-resilient hierarchical data aggregation that is designed for resilient hierarchical data aggregation in the presence of compromised nodes. In this algorithm, a portion of the total number of sensor nodes in the network generates a message authentication code (MAC) along with their sensed data as a response to the query. These MACs and the sensed data are routed to the base station that is computed at each aggregator node in the hierarchy. The base station estimates the final aggregate value accurately by verifying the MACs, and filters the effect of any falsified sub-aggregate attack contributed by compromised nodes proposed the verification algorithm (S. Roy *et al,* 2012) that is designed to validate the computed aggregate by the base station. This algorithm is an aggregate computation and verification algorithm, also known as verification algorithm. The key observation in this algorithm is to minimize the communication overhead.

This algorithm is used to verify the correctness of the aggregate of the entire network. There is no need for the base station to receive authentication messages from all nodes. The goal of this algorithm is to detect the falsified sub-aggregate attack generated by any compromised node. Algorithm involves two phases: first.: Query Dissemination: In this phase, the base station broadcasts a random number Seed, the aggregate name to compute and the chosen value of test length. In this phase, a set of the ring is formed around the base station by the nodes based on their distance in hops. Second: Aggregation Phase: Each node sends some authentication messages and executes the aggregation phase.

5. Comparison of Existing Schemes

Table 2 Comparison of Existing Schemes

Algorithms	Based-on	Aggregate considered	Authentication	No. of compromised nodes	Verification	Integrity
WDA	Single	General Aggregates	yes	≥1	yes	yes
SIA	Single	Median, Min, Max, Average	yes	≥1	yes	yes
SDA	Hierarchical	Count, Sum	yes	1	yes	yes
TAG	Hierarchical	Count, Sum	NO	0	NO	NO
SD	Hierarchical	Count, Sum	NO	0	NO	NO
SDAP	Hierarchical	Count, Sum	yes	≥1	yes	Yes
Othman et al	Hierarchical	General Aggregates	yes	≥1	yes	yes
Verification	Hierarchical	Count, Sum	yes	≥1	yes	yes
Roy et al	Hierarchical	Count, Sum	yes	≥1	yes	yes

Conclusion

The main goal of this paper is brief description of various SDA schemes in WSN, DA in WSNs, overview of approaches and attacks of DA, and discussed the existing scheme of SDA and their comparison. The existing secure data aggregation schemes are classified on basis of multiple and single aggregators. The multiple aggregator schemes are used for large network size, but the single aggregator scheme is used for small networks in which base station is only the aggregator, the design of single aggregator very easy, but multiple aggregator models are more difficult. However, the security to most of the DA schemes is provided by using message authentication code. Also the use of public keys and symmetric is used to achieve end to end or hop-by hop encryptions.

References

Priyanka B. Gaikwad, Manisha R. Dhage.(2015), Survey on Secure Data Aggregation in Wireless Sensor Networks, *Computing ommunication Control and Automation (ICCUBEA), 2015 International Conference* , pp. 242-246.

S. Siva Ranjani, Dr. S. Radhakrishnan, Dr. C. Thangaraj. (2014), Secure Cluster based Data Aggregation in Wireless Sensor Networks, *International Conference on Science, Engineering and Management Research,* pp. 1-6.

Kiran Maraiya, Kamal Kant, Nitin Gupta. (2011), Wireless Sensor Network: A Review on Data Aggregation, *International Journal of Scientific & Engineering Research*, Vol. 2, Issue 4, pp. 1-6.

Hevin Rajesh Dhasian, Paramasivan Balasubramanian. (2013), Survey of data aggregation techniques using soft computing in wireless sensor networks, *IET Information Security*, Vol.7, Issue 4, pp. 336–342.

Ameya S. Bhatlavande, Amol A. Phatak. (2015), Data Aggregation Techniques in Wireless Sensor Networks: Literature Survey , *International Journal of Computer Applications*, Vol.115 – No. 10, pp. 21–25.

S. Archana, A. Sara Vana Salvan. (2015), SAR Protocol Based Secure Data Aggregation in Wireless Sensor Network , *IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO),* pp1–6.

G. Padmavathi, D. Shanmugapriya. (2009), A Survey of Attacks, Security Mechanisms and Challenges in Wireless

Sensor Networks , *(IJCSIS) International Journal of Computer Science and Information Security,* Vol. 4, No. 1 & 2.

Jyoti Rajput, Naveen Garg. (2014), A Survey on Secure Data Aggregation in Wireless Sensor Network , *International Journal of Advanced Research in Computer Science and Software Engineering,* Vol. 4, Issue 5, pp407-412.

Jyoti Rajput, Naveen Garg. (2014), Data Aggregation in Wireless Sensor Network , IEEE *International Conference on Computational Intelligence and Computing Research,* Vol. 4, Issue 5, pp407-412.

Vasudha Khillan, Anish Soni. (2015), Secure Data Aggregation Protocols in Wireless Sensor Networks: A Review, *International Journal of Advanced Research in Computer Science and Software Engineering,* Vol.5, Issue 8, pp393-405.

B. Przydatek, D. Song, and A. Perrig. (2003), SIA: Secure Information Aggregation in Sensor Networks, *in proceedings of the 1st International Conference on Embedded Networked Sensor Systems,* pp. 255-265

L. Hu, D. Evans. (2003), Secure Aggregation for Wireless Networks, *in Symposium on Applications and the Internet Workshops,* pp. 384-391

H. Cam, S. Ozdemir, P. Nair, and D. Muthuavinashiappan. (2006), ESPDA: Energy-Efficient and Secure Pattern-Based Data Aggregation for Wireless Sensor Networks, *in Computer Communications, Elsevier,* Vol. 29, Issue 4, pp. 446–455

H. OzgurSanli, S. Ozdemir, and H. Cam. (2004), SRDA: Secure Reference-Based Data Aggregation Protocol for Wireless Sensor Networks, *in IEEE 60th Conference on Vehicular Technology, VTC2004-Fall,* Vol.7, pp. 4650–4654.

A. Mahimkar, T. S. Rappaport. (2004), Secure DAV: A Secure Data Aggregation and Verification Protocol for Sensor Networks, *in IEEE Conference on Global Telecommunications,* Vol. 4, pp. 2175-2179.

Y. Yang, X. Wang, S. Zhu, and G. Cao. (2008), SDAP: A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks, i*n Journal of ACM Transactions on Information and System Security (TISSEC),* Vol.11, Issue 4, Article No. 18.

Madden Samuel, Michael J. Franklin, Joseph Hellerstein, Wei Hong. (2002), TAG: A tiny aggregation service for ad-hoc sensor network, *ACM SIGOPS Operating Systems Review 36.SI,* pp 131-146.

W. Du, J. Deng, Y.S. Han and P.K. Varshney. (2003), A witness based approach for data fusion assurance in wireless sensor networks, *'IEEE Global Communications Conference (GLOBECOM)',* Vol.3, pp1435-1439.

Ben Othman S, Trad, A.; Youssef, H.; Alzaid, H. (2013),Secure Data Aggregation with MAC Authentication in Wireless Sensor Networks. *Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference* ,pp188-195

S. Roy, S. Setia, S. Jagodia. (2012), Attack Resilient Hierarchical Data Aggregation in Sensor Networks, SASN, Alexandria, ACM 200

S. Roy, M. Conti, S. Setia, and S. Jajodia, Secure Data Aggregation in Wireless Sensor Networks, *IEEE International Conference.*

Authors Profiles

Youssef Emhemmad Mohammad Youssef is presently pursuing a Ph.D. degree from Sam Higgin bottom Institute of Agriculture, Technology and Sciences (SHIATS), Allahabad, India. He is received Higher Diploma in computer technologies from The higher institute of professions overall-Aljufra-Sokna, Libya in year 2001 and M.Tech degree in computer science and engineering from (SHIATS) In year 2012, his research interests include computer network and web technologies.

Raghav Yadav, He is received Ph.D. degree from the Motilal Nehru National Institute of Technology (MNNIT), Allahabad, India. He received his M.Tech. Degree in computer science and engineering from MNNIT, Allahabad and B.E. degree in electronics engineering from Nagpur University. Mr. Yadav is currently an assistant professor at Sam Higginbottom Institute of Agriculture, Technology and Sciences (SHIATS), Allahabad, India. He has authored more than 20 research papers in national/international conferences and refereed journals. His research interests are in the field of optical network survivability, ad-hoc networks, and fault tolerance system