Research Journal of Applied Sciences, Engineering and Technology 6(5): 768-775, 2013
DOI:10.19026/rjaset.6.4117
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: August 30, 2012 Accepted: October 03, 2012 Published: June 25, 2013

Research Article

Secure Data Aggregation Using Reliable Nodes for Wireless Sensor Networks

[1, 2]M.Y. Mohamed Yacoab and [3]V. Sundaram
[1]Karpagam University, Coimbatore, India
[2]MEASI Institute of Information Technology, Chennai, India
[3]Karpagam College of Engineering, Coimbatore, India

Abstract: Generally, aggregation techniques in Wireless Sensor Networks (WSNs) are defenseless against various attacks. The aggregator and aggregated data has to be secured to assure integrity and confidentiality. In this study, we propose a secure data aggregation technique with reliable nodes using key predicate test protocol for sensor network. This technique specialize some nodes as Reliable nodes (R-nodes) to monitor the process of aggregation. Initially, for each node, a secret key is shared between base station and neighboring nodes. Then, an aggregation tree is constructed for transmitting data to the base station in a hierarchical fashion. The aggregator encrypts the data using secret key and forwards to a level up aggregator in aggregation tree. By enhancing broadcasting feature of R-nodes, the aggregated value is verified for ensuring integrity. As keys are shared between neighboring nodes, the nodes are validated using self-key predicate test. The proposed technique is proved through simulation results. It increases the throughput by reducing the packet drops significantly.

Keywords: Data aggregation, integrity, reliable nodes, secret key, transmission

INTRODUCTION

Wireless sensor networks: A wireless sensor network is an upcoming technology, which is being given major consideration by the research community. Several small, low cost devices constitute the sensor network, which is actually a self-organizing ad-hoc system. Its main function is to monitor the physical environment and consequently collects and dispatch information to one or more sink nodes (Dorottya and Attila, 2007). In wireless sensor network, the main operations performed are related to monitoring the physical environment, sensed information processing and result delivery to the particular sink nodes. To perform these tasks, the sensor nodes are powered by the batteries, which are resources of limited energy. Hence, designing an energy efficient protocol for increasing the network lifetime is the major dispute in this energy-constrained system (Cunqing and Tak-Shing, 2008).

Because of optimistic features of WSN, it is widely utilized in more applications such as home automation, medical applications, environmental monitoring, wildfire detection, traffic regulation and so on (Tamer and Daehun, 2009; Rodrigo and Javier, 2009; Jacques *et al*., 2010a; Suat and Yang, 2009).

Data aggregation: A common function of sensor networks is data gathering. In data gathering, the information sampled at sensor nodes desires to be transported to the central base station for further processing and analysis. An important topic mentioned by the wireless sensor networks community is the in-network data aggregation while focusing on the severe energy constraints of the sensor nodes and the limited transport capacity of multi-hop wireless networks. One of the basic distributed data processing procedures in the wireless sensor networks is data aggregation. It is used to save the energy and to reduce the medium access layer contention (Zhenzhen *et al*., 2007).

It involves merging the data from various sources along the route avoiding the redundancy, reducing the transmission numbers and hence saving the energy (Bhaskar *et al*., 2002). The efficiency and effectiveness of the sensor network can be improved considering data aggregation (Bartoli *et al*., 2010). Availability, confidentiality and flexibility are the important virtues offered by data aggregation (Tamer and Daehun, 2009).

In the dynamic scenarios, the benefits of the data aggregation can be compensated by the overhead of construction and maintenance of the structure. Some distributed approaches assume that there is a well-defined centre of event and the measured signal strength indicates the distance to the centre of the event. However, such approaches are not applicable for the applications with unstructured events like biological hazard, chemical hazard or fire detection, absence of an explicit center or any evident point of optimal aggregation (Kai-Wei *et al*., 2007).

Corresponding Author: M.Y. Mohamed Yacoab, Karpagam University, Coimbatore, India

Kinds of attacks on WSN aggregation:

- **Denial of Service attack (DoS):** It is familiar attack in wireless sensor networks that impede the radio frequencies by transmitting the radio signals in transmitting medium. This is generally referred as jamming. From the context of aggregation, DoS can take the form of aggregator that decline to aggregate the sensed data. Thereby, it makes the node not to reach the destination.
- **Sybil attack:** In Sybil attack, the attacker disseminates multiple identities of the compromised node. By generating multiple identities, the attacker makes a way to give additional votes for malicious aggregator in aggregator selection process and elects the malicious node as an aggregator. This attack induces to the worst condition of network.
- **Selective forwarding attack:** In this attack, an adversary controls the forwarded and received messages in WSN by compromising a node.
- **Replay attack:** In this kind of attack, an invader keeps track of network traffic at some part and later replays them in different part of the network. This attack misinforms the aggregator and thereby result will be exaggerated (Padmavathi and Shanmugapriya, 2009; Hani *et al*., 2008)

Security requirements in sensor networks:

- **Data integrity:** Reliability of data in sensor network can be assured by data integrity. In other words, data integrity is the process of authorizing that the transmitted message is not altered, changed or tampered by the third party.
- **Data confidentiality:** Data confidentiality is the capability of the network to cover up the transmitting message from the adversary over the communication channel. It helps to transmit the message confidentially.
- **Data authentication:** By identifying the origin of message, the authentication process assures the reliability. Generally, it is achieved by sharing secret keys through symmetric and asymmetric mechanisms.
- **Data availability:** Data availability verifies the ability of the nodes to use resources and it determines whether the network is available to transmit messages. For maintaining an operational network, determining availability plays an important role.
- **Data accuracy:** It refers to the correctness of aggregated data. Data accuracy is an important criterion for aggregating data in aggregation scheme (Padmavathi and Shanmugapriya, 2009; Hani *et al*., 2008; Zhijun and Guang, 2008).

Problem identification: In Wireless Sensor Networks (WSNs), the process of data aggregation is vulnerable to more security threats. An ideal data aggregation technique must provide reliability and fault tolerance at hand. Further, in our previous study (Mohamed Yacoab and Sundaram, 2010) we have proposed a cost effective compressive data gathering technique to enhance the traffic load, by using structured data aggregation scheme. The use of compressive data gathering provides a compressed sensor reading to reduce global data traffic and distributes energy consumption evenly to prolong network lifetime. However, our cost effective data aggregation technique does not provide any insight for reliability and fault tolerance.

In order to provide reliability and fault tolerance in data aggregation technique, as an extension to our previous work (Mohamed Yacoab and Sundaram, 2012), in this study we propose to develop a secure data aggregation technique with reliable nodes using key predicate test protocol for sensor networks.

LITERATURE REVIEW

Prakash *et al*. (2009) have proposed privacy-preserving data aggregation scheme for additive aggregation functions. The Cluster-based Private Data Aggregation (CPDA) leverages clustering protocol and algebraic properties of polynomials. The objective of their approach is to bridge the gap between collaborative data collection by wireless sensor networks and data privacy. And their approach has the advantage of incurring less communication overhead.

Jacques *et al*. (2010b) have proposed a secure end-to-end encrypted-data aggregation scheme, which is based on elliptic curve cryptography that exploits a smaller key size. Additionally, their scheme allows the use of higher number of operations on cypher-texts and prevents the distinction between two identical texts from their cryptograms. Further, their proposed approach permits the generation of shorter encryption asymmetric keys, which is so important in the case of sensor networks.

Claude *et al*. (2009) have introduced a simple and provably secure encryption scheme that allows efficient additive aggregation of encrypted data. The security of their scheme is based on the indistinguishability property of a Pseudorandom Function (PRF), a standard cryptographic primitive. To protect the integrity of the aggregated data, they have constructed an end-to-end aggregate authentication scheme that is secure against outsider-only attacks. Their proposed technique is well suitable for computing statistical values, such as mean, variance and standard deviation of sensed data, while achieving significant bandwidth savings.

Shih-I *et al*. (2009) have proposed a secure encrypted-data aggregation scheme for wireless sensor networks. Their proposed approach for data aggregation

eliminates redundant sensor readings without using encryption and maintains data secrecy and privacy during transmission. And the advantage of their proposed scheme provides security and privacy and duplicate instances of original readings will be aggregated into a single packet.

Suat and Hasan (2010) have proposed a Data Aggregation and Authentication protocol, called DAA. Their DAA is proposed to integrate false data detection with data aggregation and confidentiality. And to support data aggregation along with false data detection, the monitoring nodes of every data aggregator conduct data aggregation and compute the corresponding small-size message authentication codes for data verification at their pair mates. And supports the confidential data transmission, the sensor nodes between two consecutive data aggregators verify the data integrity on the encrypted data rather than the plain data.

Xiaodong *et al*. (2010) have proposed a multidimensional privacy-preserving data aggregation mechanism for improving security and saving energy consumption in Wireless Sensor Networks (WSNs). Their mechanism integrates the super-increasing sequence and perturbation techniques into compressed data aggregation and has the ability to combine more than one aggregated data.

Zhijun and Guang (2010) have proposed a succinct and practical secure aggregation protocol by combining HMAC (associated with a cryptographic hash function) with Bloom filter, which then is defined as secure Bloom filter. Their approach is an effective aggregation protocol that is suitable for a specific but popular class of aggregation in wireless sensor networks. The advantage from secure Bloom filter, the protocol, without any unrealistic assumptions, fulfills the fundamental security objective of preventing outside adversaries and compromised inside nodes from harming the overall network result.

Roberto *et al*. (2009) have proposed a protocol, which is based on the concept of delayed aggregation and peer monitoring and requires local interactions only. And this protocol provides both confidentiality and integrity of the aggregated data so that for any compromised sensor in the WSN the information acquired could only reveal the readings performed by a small, constant number of neighboring sensors of the compromised one and detects bogus data injection attempts and provides high resilience to sensor failures.

Haifeng (2009) has proposed a tree-sampling algorithm that directly uses sampling to answer aggregation queries and provides qualitatively improved functionality compared to existing secure aggregation protocols. The main advantage is that it solves a key challenge sampling, reducing the linear overhead to logarithmic overhead. Their protocol then leverages the nice/clean security property of sampling to achieve end goal. In addition, they have proposed a set sampling technique to overcome a key and well-known obstacle in sampling. However, their technique is only effective when the predicate count or sum is large.

METHODOLOGY

Overview: In this study, we propose to implement a secure data aggregation technique with reliable nodes using key predicate test protocol for sensor networks. Our technique specialize some nodes as reliable nodes (R-nodes) to verify the process of aggregation. Initially, each node generates a pair wise key using stream cipher technique and shares between the base station and neighboring nodes. The aggregation tree is constructed to transmit data to the base station in a hierarchical fashion. The aggregated data is encrypted using secret key and forwards to a level up in an aggregation tree. Before forwarding data to the next aggregator, the aggregated value is compared with locally aggregated data by R-nodes. If compared data is same then the data is valid and the nodes are not malicious. Conversely, when the compared data is not equal, then the data is not valid and we can conclude that nodes are compromised by the attacker. As secret key is shared between neighboring nodes, there is a chance of nodes to be compromised by the attacker. Hence, nodes with key are secured using self-key predicate test. Node that satisfies predicate test are marked as red and other nodes as yellow. The marked yellow nodes are isolated from data aggregation and transmission.

Network architecture: Consider the sensor network distributed with n number of sensing nodes. Each node senses different events. The sensed data are aggregated and transmitted to the Base Station (BS) hierarchically. Tree based approach is used for data aggregation and tree is constructed as per tree construction algorithm given in our previous study (Mohamed Yacoab and Sundaram, 2010). The tree structure is shown in Fig. 1. Presume that sensors are equipped with loosely synchronized clocks; since, data aggregation requires all nodes to transmit data to BS within some random sample period.

During the deployment of nodes in the network, we have marked a set of nodes as R-nodes (Reliable nodes). We assume that the selected R-nodes are error free and cannot be compromised by any adversaries. In this study, the selected R-nodes are responsible for monitoring the neighbor nodes for any malicious activity. Further, R-nodes are employed to validate the aggregation process.

Secure key generation and distribution: In this phase, assume that each node generates a key stream using

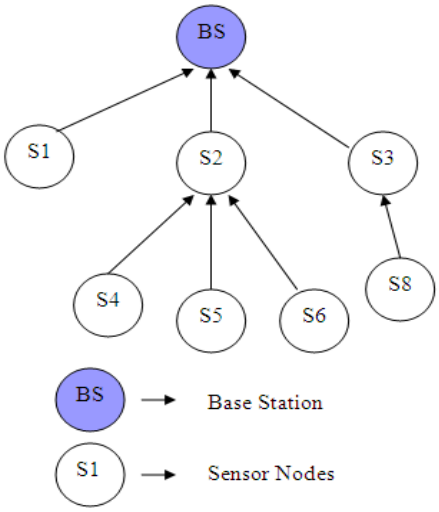

Fig. 1: Aggregation tree structure

SNOW (Patrik and Thomas, 2002), which is a new stream cipher technique. The computed secret key SK_i is shared with Base Station (BS) and also with neighboring nodes. The pair wise key distribution technique such as Dijiang and Deep (2007) is used to share the SK_i with neighbors.

As sensor nodes are vulnerable to more security attacks, data that are transmitted over the network are protected by means of homomorphic encryption scheme. Consider *PE* () as probabilistic encryption scheme. Let D be the data or message that is to be transmitted and SK_i be the secure key. Then, for any event in sensor network, the encryption scheme *PE* () can be given using modulus function *m* as:

$$PE (D1, SK1, m) = D1 + SKI (mod m) \quad (1)$$

where, *m* is modulus function on which the sum is computed and the modular function is relatively small. This encryption scheme supports additive homomorphic encryption operation. Thus, the probabilistic encryption *PE* () can be described as follows:

$$\begin{aligned} &PE (D1, SK1 m) + PE (D2, SK2, m) \\ &= (D1 + SK1 + SK1 (mod m)) + (D2 + SK2 \\ &+ (mod m)) = D1 + D2 + SK1 + SK2 (mod m) \\ &= PE (D1 + D2, SK1 + SK2, m) \end{aligned} \quad (2)$$

Aggregation with R-nodes: In our hierarchical tree based aggregation technique, each node can be either an aggregator (A_i) or an R-node. An A_i collects data from many sensor nodes (S_i) in level *a* of aggregation tree and forwards to an A_i of level *a+1*. In simple, the sensed data is transmitted from low level to the high level of the aggregation tree to reach the root. The Base Station (BS) is the root.

In addition to an aggregator (A_i) and R-node, we define another kind of node known as provider nodes (P_i), It is the set of nodes from where the aggregators (A_i) collects the information. Each provider node (P_i) encrypts the sensed data using its secret key SK_i and forwards it to the aggregator.

At time interval t, from every provider node P_i (i = 1, 2 … n), the data received by the aggregator will be in the format of three fold as (E_{Pi}, R_{Pi}, N_{Pi}).

where,
E_{Pi} = Encrypted sensed value of provider P_i
R_{Pi} = Received aggregate value of P_i
N_{Pi} = Number of provider nodes that generates corresponding aggregate value

After the expiration of time interval t, the aggregator A_i, discloses the three fold aggregated data received from every provider. By adding the data received from every provider node, it generates the new aggregated value NA_i. The NA_i is generated as follows:

$$NA_i = \frac{\sum_{p=1}^{n} (R_{pi} * N_{pi}^{-1}) + \sum_{p=1}^{n} E_{Pi}}{n} \quad (3)$$

where, n denotes the number of providers and can be represented as $n = n_{p1} + n_{p2} + \ldots + n_{pn}$.

During the computation of NA_i at time interval *t*, there is possible of taking place two circumstances as follows:

- All provider nodes (P_i) at level *a* can transmit data to aggregator A_i
- Some provider nodes at level *a* will not transmit its data to aggregator A_i

The second circumstance can happen only when communication had not taken place during that particular time interval. In such cases, the aggregator A_i adds Secret Keys (SK_i) of those sensors with new aggregate function. Then the NA_i is encrypted using nonce value (*N*) and number of providers (*n*). Ultimately, the aggregator A_i forwards NA_i to the aggregator up in the hierarchy.

Construction of R-node set: The process of R-nodes is to verify the correctness of aggregation function performed by the aggregators. The snap shot of network with R-nodes is shown in Fig. 2.

R-node set is constructed during the construction of aggregation tree topology. The R-node set of aggregator A_i is denoted by $\Re(A_i)$. It includes the neighboring nodes of A_i, which are not take part in aggregation tree. The set $\Re(A_i)$ is made known to A_i and all R-nodes.

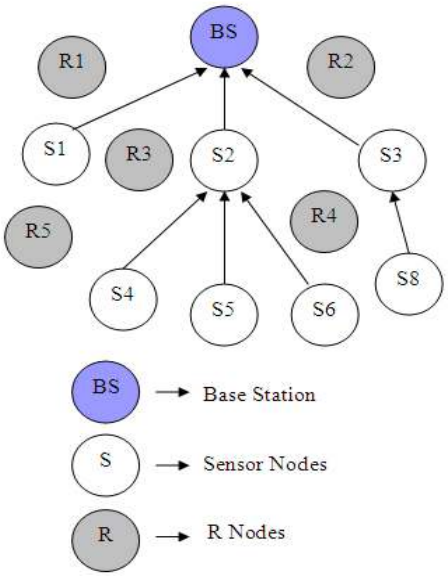

Fig. 2: Network with R-nodes

Our technique presupposes that the provider nodes of A_i are also made known to all R-nodes.

As one of the features of sensor node is radio broadcast nature, each R-node can overhear the operation done by its neighboring node. When we make use of this feature in aggregators, each R-node can aggregate the same data aggregated by its neighboring aggregators. Therefore, this overhearing feature help R-nodes to verify the aggregation process.

When A_i is aggregating data, its corresponding R-node performs the same aggregation and after time interval t, the aggregated value of A_i and R_i are compared. If the value aggregated by both A_i and R_i are same, then the verification is successful and the nodes are not malicious. On the other hand, if aggregated values are not equal then verification is unsuccessful and we can conclude that some nodes are malicious.

Algorithm-1:

Let NA_i be the aggregated value of A_i
Let R_i be the reliable node of A_i and NR_i be the aggregated value of R_i
(1) If ($NA_i = NR_i$)
Then
(i) Verification is successful
(ii) Nodes are not malicious
Else
(i) Verification is unsuccessful
(ii) Nodes are malicious
End if

In the case when provider nodes of A_i are within the range of R_i, then aggregation verification process will follow the procedure given above. When R-node does not have direct communication (within transmission range) with provider nodes of A_i, then R_i performs the aggregation within atmost two hops.

Self-key predicate test: As we discussed in section 'secure key generation and distribution', each node includes SK_i and it is shared between base station and neighboring nodes. Since, the key SK_i is shared with neighboring nodes, there is possible of an attacker to compromise a node and exploits other nodes key. Thus, the key must be verified periodically by the BS. To achieve this, the BS makes use of predicate test termed as self-key predicate test.

A predicate is a function that is stably computable, it can be denoted as P: $\chi \rightarrow \{p, q\}$. Our technique considers the non-semi linear predicate to predicates the keys of nodes. The common predicate can be given as:

$$P(S_p) = P(S_q) \quad (4)$$

where,
p & q : Input symbols
S : The number of sensors initialized in the network with symbols p and q

Our approach takes red and yellow colors as two input symbols. Based on predicate results, nodes are marked with colors. Node that satisfies the predicate are marked by red color and nodes that did not satisfy the predicate are marked with yellow color.

Initially, nodes are unmarked and nodes holding key SK_i must satisfy the predicate. Assume, each sensor has unique name in accordance with their key. Instead of using the key explicitly, the BS makes use of unique key name. As the first step of predicate test, the BS broadcasts predicate message to all nodes in the network. The predicate message includes unique name of key SK_i, the predicate, Nonce (N) and Message Authentication Code (MAC) of N:

$$\text{Base Station} \xrightarrow{\text{Predicate message}} \text{All nodes}$$

The trust worthy sensors that holds key and satisfies predicate will forward back reply to the BS. Nodes that transmit reply are marked as Red color and these nodes are valid sensors. After broadcasting predicate message, the BS will wait for *l* time, after the expiration of timer, it mark nodes that do not send reply with yellow color. The snapshot of network after self-key predicate test is given in Fig. 3.

In Fig. 3, we can see the network diagram after self-key predicate test. Nodes that are marked with red color are included in the process of aggregation and data transmission. On the other hand, nodes with yellow color are excluded from data aggregation and data transmission.

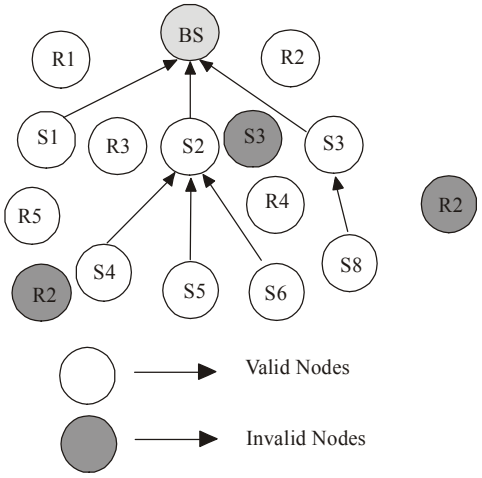

Fig. 3: Self-key predicate test

Merits of our proposed technique:

- By making use of R-nodes, our technique finds subversive activity and malicious nodes as early as possible.
- Since, aggregated data is verified with locally generated value of R-nodes; accuracy of data is assured.
- As keys of nodes are validated by self-key predicate test, there is no possible for compromising keys of nodes.
- Data is transmitted securely over the communication medium by encrypting data with homomorphic encryption technique.
- Our keying mechanism requires very less control messages to be transmitted to and fro of nodes and base station. Thus, induce very less communication overhead.

SIMULATION RESULTS

Simulation Setup: Secure Data Aggregation using Reliable nodes (SDAR) technique is evaluated through NS2 (Network Simulator, NS-2) random network deployed in an area of 500×500 m is considered. The number of nodes is kept as 100. Initially the nodes are placed randomly in the specified area. The base station is assumed to be situated 100 m away from the above specified area. The initial energy of all the nodes is assumed as 10.1 joules. 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. Table 1 summarizes the simulation parameters used.

Table 1: Simulation parameters

No. of nodes	100
Area size	500×500
Mac	802.11
Simulation time	50 sec
Traffic source	CBR
Packet size	512
Transmit power	0.660 w
Receiving power	0.395 w
Idle power	0.035 w
Initial energy	10.1 J
Transmission range	75 m
No. of sinks	2
No. of sources	4
No. of aggregator nodes	6
No. of attackers	2, 4, 6, 8 and 10

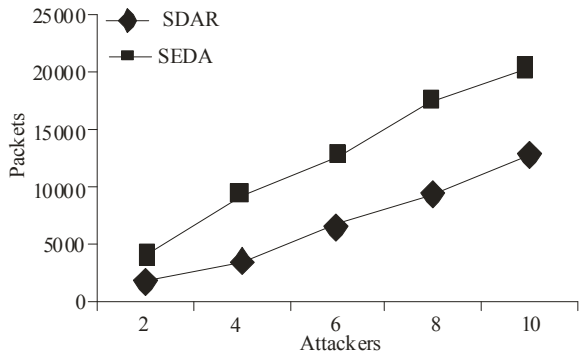

Fig. 4: Attackers Vs drop

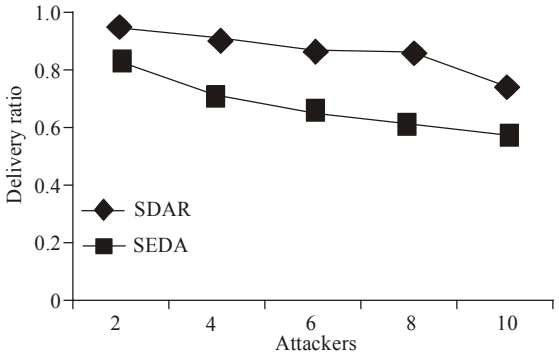

Fig. 5: Attackers Vs delivery ratio

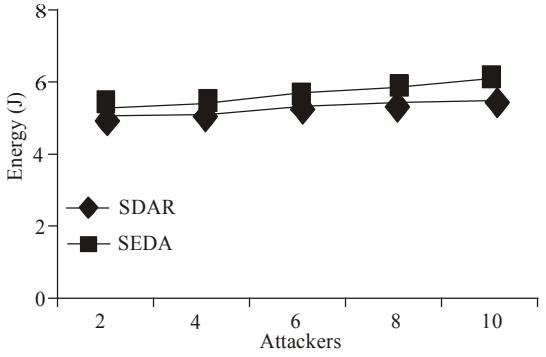

Fig. 6: Attackers Vs energy

Performance metrics: The performance of proposed SDAR technique is compared with the Secure Encrypted Data Aggregation (Shih-I *et al*., 2009) protocol. The performance is evaluated mainly, according to the following metrics.

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

Energy consumption: It is the average energy consumed by all the nodes in sending, receiving and forwarding operations

Packet drop: It is the average number of packets dropped at the receiver due to malicious attacks.

The simulation results are presented in the next section.

Results:

Based on attackers: In our initial experiment, we vary the number of attackers as 2, 4, 6, 8 and 10.

When the attackers are increased from 2 to 8, the packet drop due to the attacks will increase, as we can see from Fig. 4. But we can see that Packet drop of our proposed SDAR protocol is less than the SEDA protocol, since the data is monitored by R-nodes and protected by the aggregators.

As packet drop is increasing, the packet delivery ratio is decreasing, when the attackers are increased. From Fig. 5, we can see that the packet delivery ratio of out proposed SDAR protocol is higher than the SEDA protocol.

From Fig. 6, we can see that the Energy consumption of our proposed SDAR protocol is slightly less than that of SEDA protocol, because of the multiple sink based data gathering approach.

CONCLUSION

In this study, we have presented a secure data aggregation technique with reliable nodes using key predicate test protocol for sensor network. Our technique specialize some nodes as reliable nodes (R-nodes) to monitor the process of aggregation. Initially, for each node, a secret key is shared between base station and neighboring nodes. Then, an aggregation tree is constructed for transmitting data to the base station in a hierarchical fashion. The aggregator encrypts the data using secret key and forwards to a level up aggregator in aggregation tree. By enhancing broadcasting feature of R-nodes, the aggregated value is verified for ensuring integrity. As keys are shared between neighboring nodes, the nodes are validated as valid and invalid nodes using self-key predicate test. Our technique has proved through simulation results. It increases the packet delivery ratio by reducing the packet drops significantly.

REFERENCES

Bartoli, A., J. Hern´andez-Serrano, M. Soriano, M. Dohler, A. Kountouris and D. Barthel, 2010. Secure lossless aggregation for smart grid M2M networks. 1st IEEE International Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, MD, pp: 333-338.

Bhaskar, K., E. Deborah and W. Stephen, 2002. The impact of data aggregation in wireless sensor networks. Proceedings of IEEE 22nd International Conference on Distributed Computing Systems, (ICDCSW '02), Washington, DC, USA, pp: 575-578.

Claude, C.I., C.F.C. Aldar and M. Einar, 2009. Efficient and provably secure aggregation of encrypted data in wireless sensor networks. J. ACM T. Sensor Netw., 5(3).

Cunqing, H. and P.Y. Tak-Shing, 2008. Optimal routing and data aggregation for maximizing lifetime of wireless sensor networks. IEEE/ACM T. Networking, 16: 892-903.

Dijiang, H. and M. Deep, 2007. Secure pairwise key establishment in large-scale sensor networks: An area partitioning and multi-group key predistribution approach. J. ACM T. Sensor Networks (TOSN), 3(3).

Dorottya, V. and V. Attila, 2007. Distributed data aggregation with geographical routing in wireless sensor networks. IEEE International Conference on Pervasive Ser., pp: 68-71.

Haifeng, U., 2009. Secure and highly-available aggregation queries in large-scale sensor networks via set sampling. Proceedings of the 2009 International Conference on Information Processing in Sensor Networks, (IPSN '09), Washington, DC, USA, pp: 1-12.

Hani, A., E. Foo and N.J.M. Gonzalez, 2008. Secure Data Aggregation in Wireless Sensor Network: A survey, Australasian Information Security Conference in Research and Practice in Information Technology (CRPIT), 81, Wollongong, Australia.

Jacques, M.B., G. Christophe and M. Abdallah, 2010a. Secure data aggregation in wireless sensor networks homomorphism versus watermarking approach. ADHOCNETS, 2nd International Conference on Ad Hoc Network, Canada.

Jacques, M.B., G. Christophe and M. Abdallah, 2010b. Efficient and robust secure aggregation of encrypted data in sensor networks. 10th Proceeding of the 2010 4th International Conference on Sensor Technologies and Applications, (SENSORCOMM), Washington, DC, USA, pp: 472-477.

Kai-Wei, F., L. Sha and S. Prasun, 2007. Structure-free Data aggregation in sensor networks. IEEE T. Mobile Comput., 6(8): 929-942.

Mohamed Yacoab, M.Y. and S. Sundaram, 2010. A cost effective compressive data aggregation technique for wireless sensor networks. Int. J. Ad Hoc Sensor Ubiq. Comput. 1(4).

Mohamed Yacoab, M.Y. and V. Sundaram, 2012. Fault management for efficient data gathering in wireless sensor networks. Res. J. Appl. Sci. Eng. Technol., 4(23): 5097-5107.

Padmavathi, G. and D. Shanmugapriya, 2009. A survey of attacks, security mechanisms and challenges in wireless sensor networks. Int. J. Comput. Sci. Info. Security, 4(1-2).

Patrik, E. and J. Thomas, 2002. A new version of the stream cipher. Proceeding of the 9th Annual International Workshop on Selected Areas in Cryptography, (SAC '02), Springer-Verlag London, UK, pp: 47-61.

Prakash, G.L., M. Thejaswini, S.H. Manjula, K.R. Venugopal and L.M. Patnaik, 2009. Secure data aggregation using clusters in sensor networks: World academy of science. Eng. Technol., 51.

Rodrigo, R. and L. Javier, 2009. Integrating wireless sensor networks and the internet: A Security analysis. Internet Res., 19: 246-259.

Roberto, D.P., M. Pietro and M. Refik, 2009. Confidentiality and integrity for data aggregation in WSN using peer monitoring. Security Commun. Networ., 2: 181-194.

Shih-I, H., S. Shiuhpyng and J.D. Tygar, 2009. Secure Encrypted-Data Aggregation for Wireless Sensor Networks. Science, Business Media, LLC, Springer.

Suat, O. and X. Yang, 2009. Secure data aggregation in wireless sensor networks: A comprehensive overview. Elsevier Comput. Netw., 53: 2022-2037.

Suat, O. and C. Hasan, 2010. Integration of False data detection with data aggregation and confidential transmission in wireless sensor networks. IEEE ACM T. Networ., 18(3): 736-749.

Tamer, A. and N. Daehun, 2009. A Dynamic Level-Based Secure Data Aggregation in Wireless Sensor Network. Information Security Research Laboratory, Graduate School of IT and Telecommunication.

Xiaodong, L., L. Rongxing and S. Xuemin, 2010. MDPA: Multidimensional privacy-preserving aggregation scheme for wireless sensor networks. Wireless Communication Mobile Comput., 10(6): 843-856.

Zhenzhen, Y., A.A. Alhussein and A. Jing, 2007. Optimal policies for distributed data aggregation in wireless sensor networks. IEEE 26th IEEE International Conference on Computer Communications, (INFOCOM 2007), pp: 1676-1684.

Zhijun, L. and G. Guang, 2008. A Survey on Security in Wireless Sensor Networks. Retrieved from: http://www.cacr.math.uwaterloo.ca/techreports/2008/cacr2008-20.pdf.

Zhijun, L. and G. Guang, 2010. On data aggregation with secure bloom filter in wireless sensor networks. Technical Report CACR 2010-22, University of Waterloo, Waterloo, Ontario, Canada.