Asian Journal of Information Technology 12 (7): 208-216, 2013
ISSN: 1682-3915

A Secure and Fault-Tolerant Routing Protocol Based on GDDA and HLUA

[1]A. Gopi Saminathan and [2]S. Karthik
[1]Faculty of Electronics and Communication Engineering,
Anna University-University College of Engineering Dindigul, Dindigul, India
[2]Department of Computer Science and Engineering, SNS College of Technology,
Saravanampatti Post, Coimbatore, India

Abstract: Data aggregation protocols are required in Wireless Sensor Networks (WSNs) to extend the network lifetime by reducing the energy consumption. The existing DAO-LEACH (Data Aggregation-Optimal LEACH) protocol for WSN is insecure and prone to false data injection. This is enhanced in terms of security and fault-tolerance based on Gracefully Degraded Data Aggregation (GDDA) to ensure the integrity of the aggregated data and Hybrid Layer User Authentication (HLUA) to ensure the confidentiality of the aggregated data. This data aggregation scheme rejects the false data from compromised and malfunctioning Sensor Nodes (SNs). HLUA consists of a combination of Secret Key Cryptography (SKC) Method such as MAC (Message Authentication Code) algorithm and Public Key Cryptography (PKC) Method such as Elliptic Curve Cryptography (ECC). MAC algorithm is used between the Cluster Heads (CHs) and SNs to fulfill lower power demand while ECC is applied for User Authentication (UA) between CHs and users. The enhanced DAO-LEACH protocol is resistant to security attacks such as replay attacks, node compromising attacks and impersonation attacks. It performs better in terms of energy consumption, number of alive nodes, End to End Delay (EED) and false data detection, compared to SCAR (Simple Cluster-based data Aggregation and Routing), ESPA (Energy-efficient Secure Path Algorithm), DKS-LEACH (Deterministic Key management based LEACH), SEDAN (Secure and Efficient Data Aggregation protocol for WSNs) and DAA (Data Aggregation and Authentication).

Key words: Cluster Head (CH), Gracefully Degraded Data Aggregation (GDDA), Hybrid Layer User Authentication (HLUA), Locality Sensitivity Hashing (LSH), Low Energy Adaptive Clustering Hierarchy (LEACH), Sensor Node (SN)

INTRODUCTION

Data aggregation in Wireless Sensor Networks (WSNs) should be competent enough in terms of energy efficiency as well as security. Low Energy Adaptive Clustering Hierarchy (LEACH) protocol is considered for low energy consumption in WSN. DAO-LEACH (Data Aggregation-Optimal LEACH) protocol decreases the energy consumption in WSN compared to LEACH but it is insecure and prone to false data injection.

DAO-LEACH is enhanced in terms of security and fault-tolerance based on Gracefully Degraded Data Aggregation (GDDA) to ensure the integrity of the aggregated data and Hybrid Layer User Authentication (HLUA) to ensure the confidentiality of the aggregated data. Energy is conserved by Locality Sensitivity Hashing (LSH) technique. This data aggregation scheme rejects the false data from compromised and malfunctioning Sensor Nodes (SNs). HLUA consists of a combination of Secret Key Cryptography (SKC) Method such as MAC (Message Authentication Code) algorithm and Public Key Cryptography (PKC) Method such as Elliptic Curve Cryptography (ECC). MAC algorithm is used between the Cluster Heads (CHs) and SNs to fulfill lower power demand while ECC is applied for User Authentication (UA) between CHs and users.

The enhanced DAO-LEACH protocol is resistant to security attacks such as, replay attacks, node compromising attacks and impersonation attacks. It performs better in terms of energy consumption, number of alive nodes, End to End Delay (EED) and false data detection, compared to SCAR (simple cluster-based data aggregation and routing), ESPA (Energy-efficient Secure Path Algorithm), DKS-LEACH (Deterministic Key management based LEACH), SEDAN (Secure and Efficient Data Aggregation protocol for WSNs) and DAA (Data Aggregation and Authentication).

Corresponding Author: A. Gopi Saminathan, Faculty of Electronics and Communication Engineering,
Anna University-University College of Engineering Dindigul, Dindigul, India

EXISTING METHOD-DAO-LEACH

DAO-LEACH is a WSN routing protocol where the residual energy is considered in cluster formation and CH election. It involves a data ensemble based optimal clustering scheme where CH is termed as the aggregated node that performs data accumulation from the received cluster member data. The non-cluster nodes decide its CH based on the residual energy of the available CHs and the cluster size. Mobility of the nodes is effectively monitored and managed by a Gaussian distribution. Node aggregation is performed based on the conditional probability theorem. Gaussian distribution based nodal deployment has been applied for effective coverage of the sensing area.

Description of DAO-LEACH: The network deployment model is based on a 2D Gaussian distribution. The coverage probability is derived with respect to the Gaussian distribution. The formation of clusters in sensor network depends on the time duration for receiving the neighbor nodes message and the residual energy of the neighbor node. Two nodes do not transmit data in the same time slot in order to reduce the interference. Hop distance and hierarchy level plays the vital role in the cluster formation. The information about the neighbor nodes are gathered by broadcasting beacon messages. A sorting algorithm based on the residual energy of the neighbor nodes is executed to obtain the list of neighbor nodes regarding its hop distance.

CH performs data aggregation before transmitting the data to the sink node. Data ensemble can save considerable energy while the source nodes forming one cluster are deployed in a relatively small area when the sink node is far away from the source nodes. An election weight is determined by taking account of the concentration degree of SNs and their residual energy for optimal CH election.

A cluster of nodes in a WSN is replaced with a single node without altering the underlying joint deployment of the network. Data ensemble also takes place while aggregating the nodes. A macro node which is capable of aggregation is determined. The conditional probability of the macro node should be equal to the product of all component nodes' conditional probabilities. The conditional probability of a macro node's successor is equivalent to the conditional probability of the successor given the entire component SNs in the macro node except the nodes that are not linked directly to the successor node.

Problems in DAO-LEACH: The SNs possesses insecurity and limited energy. The sensed information is aggregated at CHs to reduce the energy consumption by decreasing the network traffic. But data aggregation puts forward security challenges like confidentiality and integrity of data. The aggregated data is exposed to intruders making the data insecure. Similarly, an unauthorized user can attach false data into the aggregated data and make the sink node accept false data.

LITERATURE REVIEW

This study deals with various methods for enhancing the security and energy-efficiency and detection of false data during data aggregation in WSN. Fukabori *et al.* (2010) proposed an energy-efficient data aggregation using the degree of cluster dependence. The energy consumption of the SNs is reduced by using the mobility of the sink node. A new routing and data aggregation scheme is used based on clustering. Mpitziopoulos *et al.* (2010) proposed a scalable technique for distributed data aggregation for reduction decreasing energy expenditure in WSNs. A novel algorithm called Clone-Based Itinerary Design (CBID) is used to determine the near-optimal routes for the Mobile Agents (MAs) in the WSN. MAs incrementally aggregate the data as they traverse the SNs while also updating the designed itineraries upon variations of network topology. Hong *et al.* (2013) evaluated the performance of a Simple Cluster-based data Aggregation and Routing (SCAR) in WSN. This method decreases the overhead incurred during CH selection in WSNs. This can achieve energy-balancing when nodes are limited in mobility. Conservation of energy prolongs the lifetime of SNs.

Sicari *et al.* (2012) proposed a dynamic secure end to end data aggregation method for ensuring the privacy of the WSNs. The design includes a UML (Unified Modeling Language) Model that includes the basic elements of a privacy-aware network including aggregation policies. The aggregation algorithm involves a discrete-time control loop for decrease of communication load and dynamic in-network data fusion. Wang *et al.* (2012) enhanced the security of the LEACH routing protocol for WSN using μTESLA and Exclusion Basis Systems (EBS). μTESLA is used for updating the security key and EBS is used for the key generation and distribution. Harjito *et al.* (2010) developed a lightweight digital watermarking method for enhancing the security of Wireless Multimedia Sensor Networks (WMSNs). WMSNs are a class of WSNs that contains SNs with cameras, microphones and other multimedia devices. This method focuses on multimedia data authentication and

privacy perseveration during compression and aggregation of multimedia data. Zhu *et al.* (2011) proposed a secure and energy-efficient data aggregation scheme for WSNs. The BS consists of a secret configuration matrix. Each SN knows a limited section of the matrix described as a secret share. The communication overhead is considerably reduced by avoiding the verification of aggregation integrity.

Bo *et al.* (2013) proposed a secure in-network data aggregation with anomaly detection in WSNs. The false injected data are detected using EKF (Extended Kalman Filter) based mechanism. Each SN characterizes a normal range of neighboring SN's future transmitted aggregated values by monitoring the neighbor behavior and using EKF for prediction of their future states. EKF is used for effective local false data detection. A combined algorithm of Generalized Likelihood Ratio (GLR) and Cumulative Summation (CUSUM) are used to enhance the detection sensitivity. This local false detection method is combined with system monitoring to distinguish between emergency events and malicious events. Energy consumption is reduced by scheduling some of the SNs to sleep periodically. Ozdemir and Cam (2010) combined a false data detection module with data aggregation for confidential transmission in WSNs (Ozdemir and Xiao, 2011). The main source of false data is compromised SNs which injects false data during aggregation and forwarding of data. Every data aggregator performs data aggregation and computes the relative MACs. The SNs between two consecutive data aggregators verify the integrity of the encrypted data. Data aggregators keep on changing between the SNs depending on their residual energy levels to decrease the energy consumption. Bagaa *et al.* (2012) proposed SEDAN (Secure and Efficient Data Aggregation protocol for WSNs) which involves a secure and energy-efficient data aggregation technique with false data detection.

Ba *et al.* (2010) proposed a deterministic key management based LEACH protocol (DKS-LEACH) for secure and energy-efficient cluster-based WSNs. Various attacks are avoided by a secure communication between SNs and CHs as well as CHs and BS. The memory usage is also decreased by using a limited number of keys. Yang *et al.* (2013) proposed a data aggregation scheme that enhances the precision and preserves the privacy mixed with encryption. This method reduces the energy consumption and collision using a data compensation algorithm and a randomized time slot during aggregated data transmission. The data slicing process is optimized by using Node Classification, Small Data Packet and ± Data Slicing Methods. Huang *et al.* (2010a) proposed a secure routing protocol using ID-based digital signature for cluster-based WSNs. This method consists of a random oracle model where the security is dependent on the hardness of the Diffie-Hellman problem. This technique uses a dynamic clustering LEACH protocol to reduce the energy consumption. SNs are selected as CHs in rounds for fair energy consumption. An integrated approach of in-network data aggregation for reducing energy consumption and two protocols namely PASKIS (Privacy-preserving based on Anonymously Shared Keys and Ignorant Sink) and PASKOS (Privacy-preserving based on Anonymously Shared Keys and Omniscient Sink) for secure data aggregation is applied (Lei *et al.*, 2010).

Several other researchers proposed secure and energy-efficient data aggregation methods. These methods involve multidimensional data aggregation (Lin *et al.*, 2010), Perturbation-based Efficient Confidentiality Preserving Protocol (PEC2P) (Zhu *et al.*, 2013), hierarchical clustering (Su *et al.*, 2012), Energy-efficient Secure Path Algorithm (ESPA) (Dieu *et al.*, 2012) and elimination of recursive sensor readings (Huang *et al.*, 2010b).

PROPOSED METHOD

The existing DAO-LEACH protocol guarantees only the energy-efficiency of WSN. This is further enhanced to affirm security and removal of false data. The integrity of the aggregated data is fulfilled by GDDA scheme and the confidentiality of the aggregated data is guaranteed by HLUA scheme.

Gracefully Degraded Data Aggregation (GDDA) scheme: This method is able to detect the false data in the sensed data and eliminate them. This ensures the fault-tolerance in the WSN. It is based on Locality Sensitivity Hashing (LSH) technique. Support values and support counts are defined for each cluster. Minimum support values for each cluster are estimated in terms of local cluster ($minSup_l$) and neighboring cluster ($minSup_n$). The working of the GDDA scheme in each cluster is given in Fig. 1.

Locality Sensitive Hashing (LSH) algorithm: Consider a s-dimensional real space $\mathbb{R}^s$ with two data points a and b. a is known as a r-near neighbor of b, since distance between a and b is less than r. LSH algorithm depends on the presence of locality sensitive hash functions. The family of hash functions mapping $\mathbb{R}^s$ to some universal set

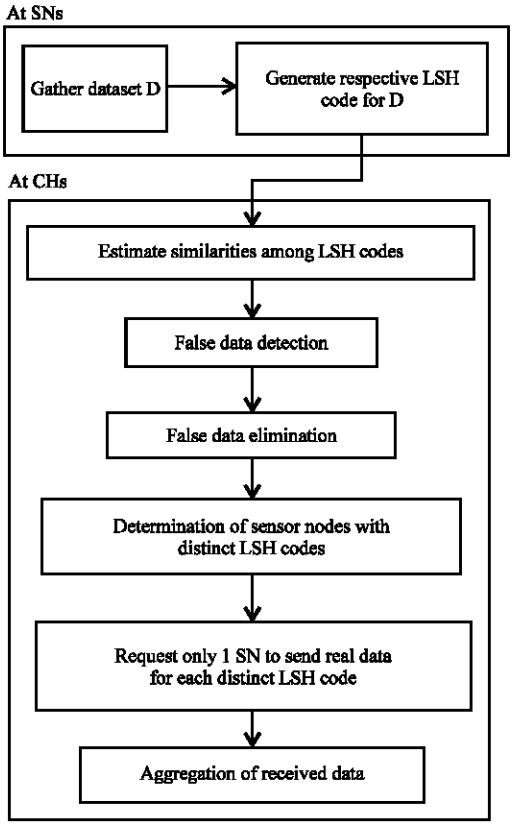

Fig. 1: Working of GDDA scheme

is denoted as $\mathcal{H}$. A sub-function in $\mathcal{H}$ is denoted as h. For data points a and b, h(a) = h(b). The family of hash functions $\mathcal{H}$ is said to be locality sensitive under the following conditions:

$$\text{If } \|a-b\| \le r \text{ then } Pr_{\mathcal{H}}[h(b) = h(a)] \ge c_1$$

$$\text{If } \|a-b\| \ge kr \text{ then } Pr_{\mathcal{H}}[h(b) = h(a)] \le c_2$$

Where:
k = A constant
c_1 = 1-(r/s)
c_2 = 1-(cr/s)

A family of hash functions must satisfy the condition $c_1 > c_2$. $\mathcal{H}$ can determine whether a and b are in the r-neighborhood of each other. Random hyperplane-based hash functions $h_{rd}(m)$, $h_{rd}(n)$ are considered with vectors (m, n)$\in \mathbb{R}^s$, rd is the random hyperplane. The vectors (m, n) give the cosine similarity metric of the data points:

$$m, n = \arccos\left(\frac{m.n}{\|m\|.\|n\|}\right) \quad (1)$$

$$h_{rd}(m) = \begin{cases} 1, & rd \times m \ge 0 \\ 0, & rd \times m < 0 \end{cases} \quad (2)$$

The probability distribution (Pr) for the vectors (m, n) is defined as:

$$Pr\left[h_{rd}(m) = h_{rd}(n)\right] = 1 - \frac{d_H(LSH_m, LSH_n)}{\pi} \quad (3)$$

$$d_H(LSH_m, LSH_n) = j.(1\text{-}Pr) = j.\frac{\theta(m,n)}{\pi} \quad (4)$$

The hash function determines the similarity between any pair of datasets in terms of angle between two vectors. Equation 4 defines the Hamming distance between the LSH codes of vectors m and n, i.e., LSH_m and LSH_n. The bit length (j) of each LSH code is much smaller than original vectors m and n. The similarity threshold (Θ) is expressed in terms of Hamming distance as:

$$\Theta_{d_H} = \frac{j\Theta}{\pi} \quad (5)$$

Data aggregation: Each SN senses the environment p times and stores the sensed values, each of q bits length. Thus, each SN has a data vector of size (p×q)-bit. Transferring this data vector to CHs results in rapid depletion of the SN's battery. LSH codes are generated by the SNs to decrease the amount of data transmitted. LSH codes are used to define the sensor data using less number of bits. LSH algorithm is used to evaluate a j-bit LSH code where $j << (p \times q)$. The false data detection accuracy increases when the values of j and (p×q) are close to each other.

Each CH requests the SNs in its cluster to transmit their LSH codes for data aggregation. The SNs append their unique IDs along with the LSH codes. Using Eq. 4 and 5, the CH compares the LSH codes of any SN pair.

Case 1 (Different LSH codes): The relation between the different pairs of LSH codes is determined by the CH based on their Hamming distance and similarity threshold Θ_{d_H}. When a LSH code is similar to the other LSH code, its support count is incremented by 1. When false data are present in the local cluster, the support count of the LSH codes is less than $minSup_l$. The CHs of the neighboring clusters exchange their local false data among themselves to determine if these false data would affect their support count. Each CH compares the LSH codes of its neighboring false data with its cluster's LSH codes. The support counts are updated after each comparison with the neighboring cluster's false data. The neighboring CHs exchange the updated support count of local false data.

Case 2 (Similar LSH codes): The CHs determine the SNs that transmitted similar LSH codes. This is used to eliminate the recursive data transmission from SNs to CHs. When more than one SN contain similar LSH codes then the CH selects only one SN among them to transfer its original data.

After the determination of false data and LSH codes, the CHs obtain the list of false data and SNs containing similar LSH codes. CHs eliminate the false data and request only one SN to send the original data for each similar LSH code. Only the requested SNs transmit their sensed data to the CH and the CH does not accept data from any other SNs. This ensures that no false data are included in the aggregated data and there is no repetitive data transmission from SNs to the CH. The CH aggregates the received data and transmits the aggregated data to the base station.

Hybrid Layer User Authentication (HLUA) scheme: CHs have high processing capability and communication power than SNs. CHs act as trusted gateways to the SNs. Public Key Cryptography (PKC) Method such as Elliptic Curve Cryptography (ECC) is applied for User Authentication (UA) between CHs and users. A user is allowed to access the SNs through the CH when it is authenticated to that CH. A Symmetric Key Cryptography (SKC) Method such as MAC (Message Authentication Code) algorithm is used between the CHs and SNs to fulfill lower power demand. In the HLUA scheme a user needs to register only once and can be authenticated to the network several times. The users can also alter their password at any time. The Base Station (BS) serves as a trusted key management center. CHs are equipped with intrusion-resistant hardware to protect the cryptographic materials. The users can access the WSN with portable computing devices like laptop for request and retrieval of data. The sensed information is processed and the SN sends the data upon the detection of an event or stores it for the purpose of the next data query.

Key agreement: A Public Key Infrastructure (PKI) executing the ECC is considered throughout the WSN. A BS acts as the certification authority for WSN and ECC is used for encryption/decryption purposes. Digital certificate generation and verification processes are carried out by Elliptic Curve Digital Signature Algorithm (ECDSA). The key agreement between a CH and its associated SNs are performed by Elliptic Curve Diffie Hellman (ECDH) key agreement protocol. The key agreement protocol computes the pairwise MAC keys ($K_{CH,\ SN}$). BS initializes the parameters for elliptic curve operations to be used by the WSN components. The parameters are denoted as follows:

- Base point X
- Private key for BS (K_{pr_BS}) and public key for BS (K_{pb_BS})
- Private key for each SN (K_{pr_SN}) and public key for each SN (K_{pb_SN})

Each public key is equivalent to the elliptic curve product of the associated private key and the base point. Each SN contains the public key of their CH and their private-public keys. Each CH contains the public key of the SNs and their private-public keys.

ECDH permits two users to accept on the secret key of the MAC algorithm. The public keys required for the ECDH protocol are exchanged between the SNs and their associated CHs before the node deployment to decrease the energy consumption. Each SN computes a secret shared key or MAC key ($K_{CH,\ SN}$) after the node deployment.

An SN computes the elliptic point P_{SN}, denoted as (x_{SN}, y_{SN}). It is equivalent to the elliptic curve product of K_{pr_SN} and K_{pb_CH}. The associated CH computes another elliptic point P_{CH}, denoted as (x_{CH}, y_{CH}). It is equivalent to the elliptic curve product of K_{pr_CH} and K_{pb_SN}.

Authentication: A user requests the BS with its ID encrypted with the BS public key for registration to the WSN. The BS contains the ID list of authenticated users, providing each authenticated user a certificate. The BS also contains a pair of private and public key (K_{pr_BS}, K_{pb_BS}). The BS uses the private key K_{pr_BS} to sign the user's ID and compose it as a certificate. The user receives the certificate from the BS. Each CH can verify the validity of the user certificate with K_{pb_BS} during the process of UA and extract the user ID (ID_u). The authentication process is explained in a flowchart as shown in Fig. 2. At the end of the authentication process, a SN may inform the user authentication via CH by a short message.

The users can change their password through the BS. The user encrypts the changed public key $K_{pb\_u}^*$ and it's changed ID (ID_u^*) with its existing public key K_{pb_u}. BS decrypts the encrypted message by using the existing public key of the user K_{pb_u}. Then, BS signs the changed ID (Id_u^*) by its private key K_{pr_BS} to estimate a changed certificate cer_u^* and transmit it back to the user.

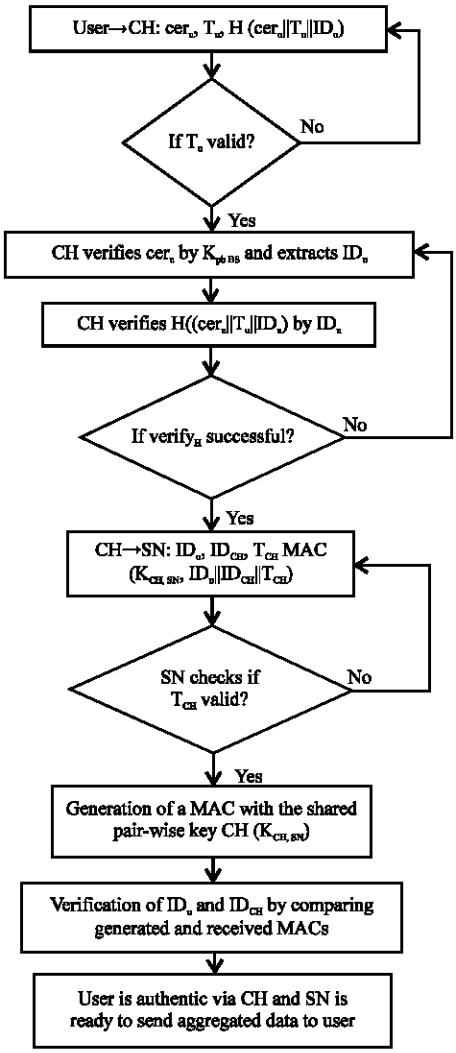

Fig. 2: Working of HLUA scheme

SECURITY ANALYSIS

PKC is chosen in the HLUA scheme due to lesser memory usage and higher security resilience. Users can be added in real-time in this method. A secure channel is not required between BS and user due to the PKI used in the HLUA Method. Thus, users don't need to be connected with BS for the exchange of keys. The users can communicate with the BS directly to change the password. The HLUA scheme is resistant to the following attacks.

Replay attacks: An intruder cannot re-use the former login message to hack the WSN because the timestamp produced by the user ensures that this message cannot be used after some time. After the limited amount of time, CH will not permit access to the user.

Node compromising attacks: The nodes cannot be compromised due to the intrusion-resistant hardware of CHs. SNs do not carry important information to compromise the entire WSN. The secret keys between each SN and its associated CH are updated at specific periods with ECDH protocol to defend against the compromising of the connection of the SN and its CH.

Impersonation attacks: An attacker with a guess ID ($ID_{u\text{-}guessed}$) tries to impersonate the login message $H(cer_u||T_u||ID_u)$. If the attacker doesn't know K_{pb_BS}, the attacker cannot verify user certificate and user ID. Therefore, $ID_{u\text{-}guessed}$ will alter the hash value and will be captured by the CH.

PERFORMANCE EVALUATION

The enhanced DAO-LEACH protocol for WSN is compared with various existing secure and energy-efficient data aggregation schemes in WSN. The network architecture consists of 500 nodes in a simulated area of 10003×1000 m. The nodal velocity is varied from 5-30 m sec^{-1}. The enhanced DAO-LEACH protocol is analyzed with existing methods like SCAR (Hong *et al*., 2013), DAA (Ozdemir and Cam, 2010), SEDAN (Bagaa *et al*., 2012), DKS-LEACH (Ba *et al*., 2010) and ESPA (Dieu *et al*., 2012) in terms of the following parameters.

Average remaining energy: The average remaining energy of the system is analyzed with respect to time and the number of packets received in enhanced DAO-LEACH, SCAR and ESPA. The analysis is given in Fig. 3. It is observed than enhanced DAO-LEACH is better than the other two methods. Initially in enhanced DAO-LEACH, the average remaining energy decreases rapidly and then stabilizes into a constant decrease over time and the number of received packets.

Average energy consumption of SN: The average energy consumption of SNs for different network size is analyzed between DKS-LEACH and enhanced DAO-LEACH and given in Fig. 4. It is observed that the average energy consumed in DKS-LEACH varies randomly while that for enhanced DAO-LEACH is a constant increase as the the number of nodes increases. The average energy consumption of SNs in enhanced DAO-LEACH is comparatively lesser than that of DKS-LEACH.

Energy consumption in system: The energy consumption in the system is analyzed between SEDAN and enhanced DAO-LEACH for different number of packets and

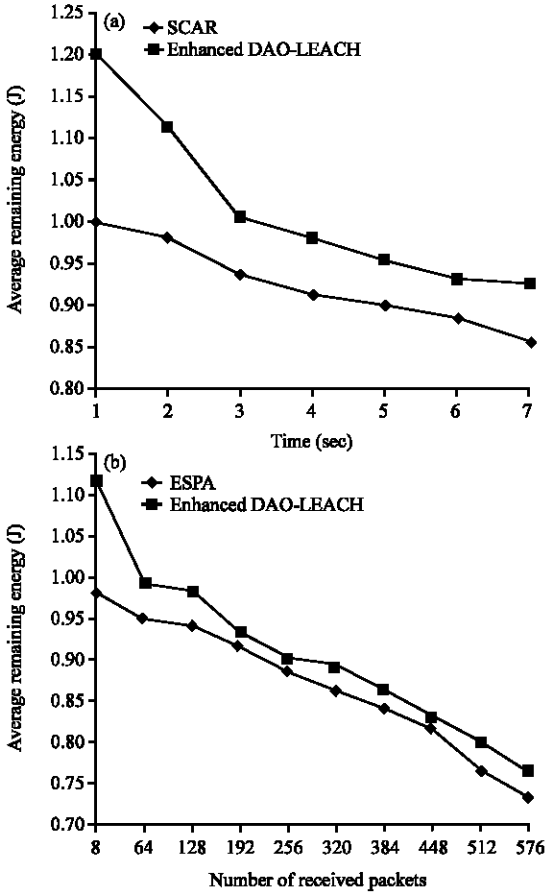

Fig. 3: Average remaining energy; a) over time and b) number of received packets

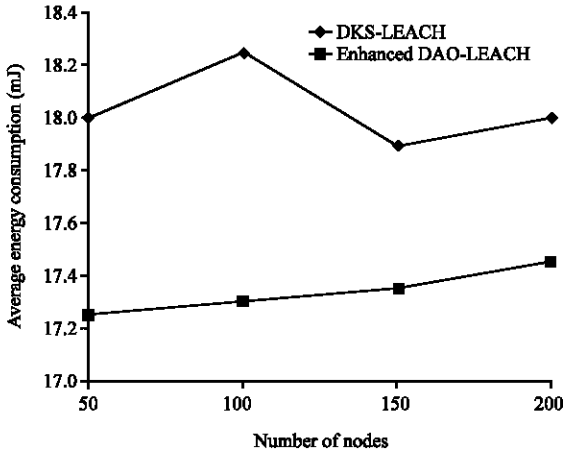

Fig. 4: Average energy consumption of SNs for different network size between DKS-LEACH and enhanced DAO-LEACH

different number of nodes in Fig. 5. It is observed that the increase in energy consumption versus the number of

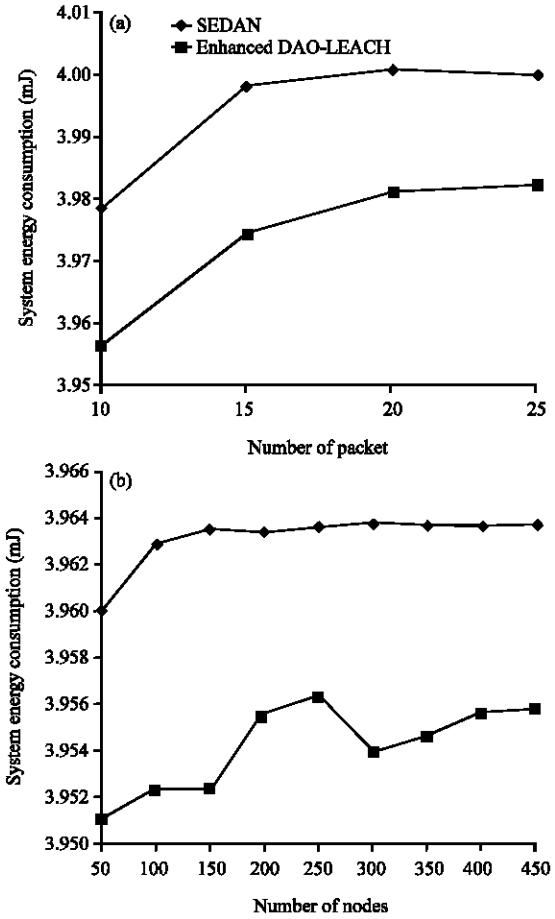

Fig. 5: Energy consumption in system versus; a) number of packets and b) number of nodes

packets follows a similar trend for both the methods. But the increase in energy consumption versus the number of nodes for enhanced DAO-LEACH is initially high and then stabilizes to a constant increase. The system energy consumption for enhanced DAO-LEACH is relatively lesser than that of SEDAN.

Number of alive nodes: The number of alive nodes per time between ESPA (with BS verification) and enhanced DAO-LEACH is analyzed in Fig. 6. Five attackers are considered for the analysis. The number of alive nodes decreases from 100. It is observed that the magnitude of decrease is greater for ESPA than that of enhanced DAO-LEACH. When there are a higher number of alive nodes, it will prolong the network lifetime.

End to end delay: The End to End Delay (EED) per number of nodes between DKS-LEACH and enhanced DAO-LEACH is analyzed in Fig. 7. EED increases constantly for

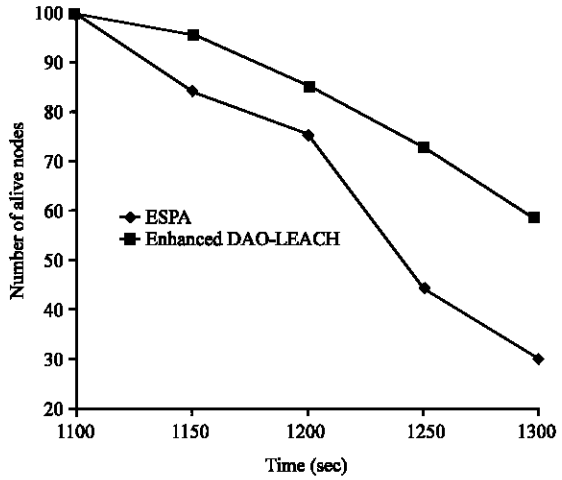

Fig. 6: Number of alive nodes per time between ESPA and enhanced DAO-LEACH

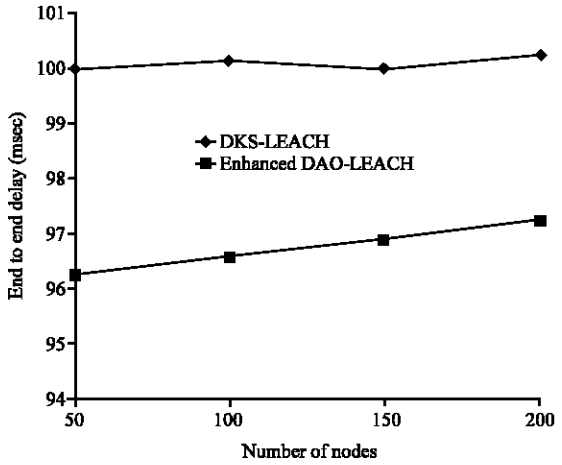

Fig. 7: End to end delay between DKS-LEACH and enhanced DAO-LEACH

enhanced DAO-LEACH as the number of nodes increases. Lesser the EED, lesser is the time taken for the encryption and decryption of messages.

False data detection: The false data detection is analyzed in terms of total transmission data and Mean Time To Detection (MTTD) between DAA, SEDAN and enhanced DAO-LEACH. The comparative analysis is given in Fig. 8. As the false data in WSN increases, the total data transmission increase. This increase should be in a steady and least manner to ensure transmission of lesser false data. MTTD is the average delay between the injection of a false data packet and its detection. Lesser is the MTTD; quicker is the detection of false data in the system. It is observed that the MTTD varies randomly in SEDAN and increases steadily in enhanced DAO-LEACH for an increasing number of nodes.

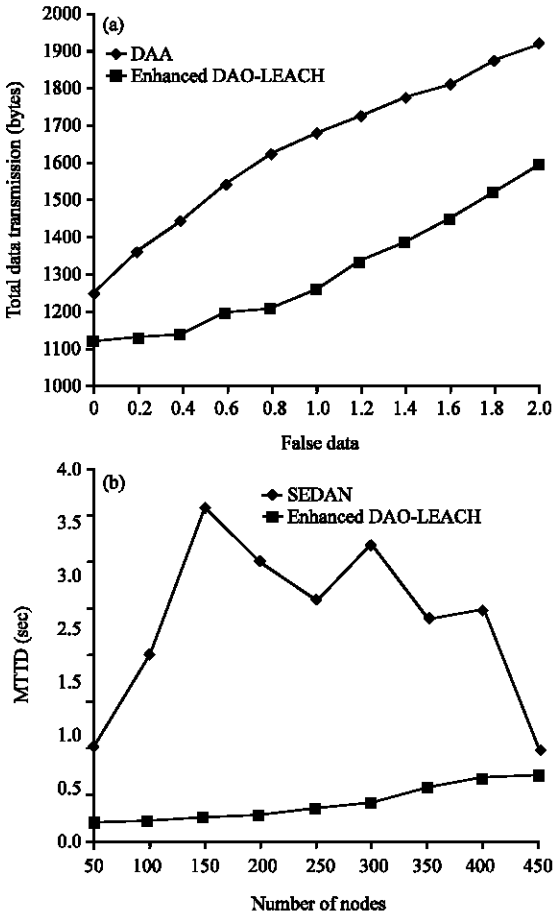

Fig. 8: False data detection analysis; a) total transmission data and b) MTTD (Mean Time To Detection)

CONCLUSION

Data aggregation and optimal clustering are incorporated in WSN to increase the energy efficiency of LEACH (Low Energy Adaptive Clustering Hierarchy) protocol, known as DAO-LEACH (Data Aggregation Optimal LEACH). The data aggregation process of DAO-LEACH is insecure and prone to false data injection. This is enhanced in terms of security and fault-tolerance based on Gracefully Degraded Data Aggregation (GDDA) to ensure the integrity of the aggregated data and Hybrid Layer User Authentication (HLUA) to ensure the confidentiality of the aggregated data. HLUA consists of a combination of Secret Key Cryptography (SKC) Method such as MAC (Message Authentication Code) algorithm and Public Key Cryptography (PKC) Method such as Elliptic Curve Cryptography (ECC).

The enhanced DAO-LEACH protocol is resistant to security attacks such as replay attacks, node compromising attacks and impersonation attacks. It performs better in terms of energy consumption, number

of alive nodes, End to End Delay (EED) and false data detection, compared to SCAR (Simple Cluster-based data Aggregation and Routing), ESPA (Energy-efficient Secure Path Algorithm), DKS-LEACH (Deterministic Key management based LEACH), SEDAN (Secure and Efficient Data Aggregation protocol for WSNs) and DAA (Data Aggregation and Authentication).

The future research of enhanced DAO-LEACH protocol for WSN involves optimization of the energy-efficient and secure routing protocol in terms of memory (bandwidth, message size per packet, data transmission), communication overhead, number of computations and aggregation accuracy.

REFERENCES

Ba, M., I. Niang, B. Gueye and T. Noel, 2010. A deterministic key management scheme for securing cluster-based sensors networks. Proceedings of the 8th International Conference on Embedded and Ubiquitous Computing, December 11-13, 2010, Hong Kong, pp: 422-427.

Bagaa, M., Y. Challalb, A. Ouadjaouta, N. Laslaa and N. Badachea, 2012. Efficient data aggregation with in-network integrity control for WSN. J. Parallel Distrib. Comput., 72: 1157-1170.

Bo, S., X. Shan, K. Wu and Y. Xiao, 2013. Anomaly detection based secure in-network aggregation for wireless sensor networks. IEEE Syst. J., 7: 13-25.

Dieu, I.J.D., N. Assouma, M. Muhamad, W. Jin and S. Lee, 2012. Energy-efficient secure path algorithm for wireless sensor networks. Int. J. Distrib. Sensor Networks, Vol. 2012. 10.1155/2012/751784.

Fukabori, T., H. Nakayama, H. Nishiyama, N. Ansari and N. Kato, 2010. An Efficient data aggregation scheme using degree of dependence on clusters in WSNs. Proceedings of the IEEE International Conference on Communications, May 23-27, 2010, Cape Town, pp: 1-5.

Harjito, B., S. Han, V. Potdar, E. Chang and M. Xie, 2010. Secure communication in wireless multimedia sensor networks using watermarking. Proceedings of the 4th IEEE International Conference on Digital Ecosystems and Technologies, April 13-16, 2010, Dubai, pp: 640-645.

Hong, S.H., J.M. Park and J.M. Gil, 2013. Performance evaluation of a simple cluster-based aggregation and routing in wireless sensor networks. Int. J. Distrib. Sensor Networks, Vol. 2013. 10.1155/2013/501594.

Huang, L., J. Li and H. Kameda, 2010a. A secure routing protocol for cluster-based wireless sensor networks using ID-based digital signature. Proceedings of the IEEE Global Telecommunications Conference GLOBECOM, December 6-10, 2010, Miami, FL., pp: 1-5.

Huang, S.I., S. Shieh and J.D. Tygar, 2010b. Secure encrypted-data aggregation for wireless sensor networks. Wireless Networks, 16: 915-927.

Lei, Z., H. Zhang, M. Conti, R. di Pietro, S. Jajodia and L.V. Mancini, 2010. Reverse tree-based key routing: Robust data aggregation in wireless sensor networks. Proceedings of the 10th International Conference on Computer and Information Technology, June 29-July 1, 2010, Bradford, pp: 910-915.

Lin, X., R. Lu and X. Shen, 2010. MDPA: Multidimensional privacy-preserving aggregation scheme for wireless sensor networks. Wireless Commun. Mobile Comput., 10: 843-856.

Mpitziopoulos, A., D. Gavalas, C. Konstantopoulos and G. Pantziou, 2010..CBID: A scalable method for distributed data aggregation in WSNs. Int. J. Distrib. Sensor Networks, Vol. 2010. 10.1155/2010/206517.

Ozdemir, S. and H. Cam, 2010. Integration of false data detection with data aggregation and confidential transmission in wireless sensor networks. IEEE/ACM Trans. Network, 18: 736-749.

Ozdemir, S. and Y. Xiao, 2011. Integrity protecting hierarchical concealed data aggregation for wireless sensor networks. Comput. Networks, 55: 1735-1746.

Sicari, S., L.A. Griecob, G. Boggiab and A. Coen-Porisinia, 2012. DyDAP: A dynamic data aggregation scheme for privacy aware wireless sensor networks. J. Syst. Software, 85: 152-166.

Su, T.S., M.W. Huang, W.S. Li and W.S. Hsieh, 2012. Aggregation scheme with secure hierarchical clustering for wireless sensor networks. Int. J. Distrib. Sensor Networks, Vol. 2012. 10.1155/2012/162347.

Wang, J., L. Zheng, L. Zhao and D. Tian, 2012. LEACH-based security routing protocol for WSNs. Adv. Comput. Sci. Inf. Eng., 169: 253-258.

Yang, G., S. Li, X. Xu, H. Dai and Z. Yang, 2013. Precision-enhanced and encryption-mixed privacy-preserving data aggregation in wireless sensor networks. Int. J. Distrib. Sensor Networks, Vol. 2013. 10.1155/2013/ 427275.

Zhu, L., Z. Yang, M. Wang and M. Li, 2013. ID list forwarding free confidentiality preserving data aggregation for wireless sensor networks. Int. J. Distrib. Sensor Networks, Vol. 2013. 10.1155/2013/ 241261.

Zhu, W.T., F. Gao and Y. Xiang, 2011. A secure and efficient data aggregation scheme for wireless sensor networks. Concurrency Comput.: Pract. Exp., 23: 1414-1430.