ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Secure and Vitality Productive Information Conglomeration in Remote Sensor Systems

Dommeti Lakshmi Prasanna
M.Tech Student
Department of Computer Science and Engineering,
Sai Madhavi Institute of Science And Technology,
Rajahmundry, A.P-533296, India.

Mr. Chinnam Yuva Raju, M.Tech, (Ph.D)
Associate Professor
Department of Computer Science and Engineering,
Sai Madhavi Institute of Science And Technology,
Rajahmundry, A.P-533296, India.

ABSTRACT

To diminish the correspondence overhead and drag out the framework lifetime data gathering is used in remote sensor frameworks. On the other hand, an adversary may deal some sensor centers, and use them to deliver false esteems as the gathering result. Past secure data aggregation designs have taken care of this issue from different focuses.

The goal of those computations is to ensure that the Base Station (BS) does not recognize any formed gathering comes about. Nevertheless none of them have endeavored to recognize the center points that mix into the framework counterfeit gathering comes about. Likewise, most of them for the most part has a correspondence overhead that is, (most ideal situation) logarithmic each center point. In this paper, we propose an ensured and imperativeness successful data add up to arrange for that can recognize the horrendous centers with an enduring each center correspondence overhead. In our answer, every aggregate outcome are set apart with the private keys of the aggregators so they can't be changed by others.

Center points on each association additionally use their combine astute granted key for secure correspondences. Each center point gets the aggregate outcomes from its parent (sent by the watchman of its parent) and its kinfolk (through its parent center point), and affirms the gathering eventual outcome of the gatekeeper center point. Theoretical examination on essentialness use and correspondence overhead agrees with our relationship based entertainment inspect over sporadic data aggregation trees.

Introduction

Remote sensor frameworks (WSFs) are getting the chance to be continuously outstanding to give answers for some security-separating applications, for instance, wild campfire following, military perception, and nation security. In sensor frameworks, a large number of sensor center points in general screen a range. As all the sensor center points in a range typically recognize consistent wonders, there is high redundancy in the unrefined data.

To save essentialness and drag out framework lifetime, a capable course is to add up to the unrefined data previously they are transmitted to the base station as the sensor center points are resource compelled and imperativeness obliged. Data collection is a key standard to discard data reiteration and decline essentialness usage. In the midst of a common data add up to strategy, sensor center points are created into a different leveled tree built up at the base station the sensor centers are routinely passed on in undermining and unattended circumstances, and are not made precisely outlined on account of cost considerations. So they might be gotten by a foe, which may self-decisively disturb the data to fulfill its own inspiration. Thusly, an essential issue in applying data accumulation is to avoid such adjusting so the base station can get the correct data combination result.

Security assurance has been widely contemplated in different fields, for example, wired and remote systems administration, databases and information mining. In any case, the accompanying inalienable highlights of WSNs present one of a kind difficulties for protection conservation of information and keep the current

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

systems from being specifically actualized in these systems. Wild condition: sensors may must be sent in a situation that is wild by the protector, for example, a front line, empowering a foe to dispatch physical assaults to catch sensor hubs or convey fake ones. Therefore, an enemy may recover private keys utilized for secure correspondence and decode any correspondence listened in by the foe. Sensor-hub asset imperatives: battery-fueled sensor hubs by and large have serious requirements on their capacity to store, process, and transmit the detected information. Therefore, the computational many-sided quality and asset utilization of open key figures is typically viewed as unacceptable for WSNs.

Topological limitations: the restricted correspondence scope of sensor hubs in a WSN requires various bounces with a specific end goal to transmit information from the source to the base station. Such a multi-bounce plot requests distinctive hubs to take various activity loads.

Specifically, a hub nearer to the base station (i.e., information gathering and preparing server) needs to hand-off information from hubs encourage far from base station notwithstanding transmitting its own particular produced information, prompting higher transmission rate. Such a lopsided system activity design conveys critical difficulties to the security of setting focused protection data. Especially, if a foe can complete a worldwide activity investigation, watching the movement examples of various hubs over the entire system, it can undoubtedly recognize the sink and trade off setting protection, or even control the sink hub to block the best possible working of the WSN.

Overview of Aggregation Protocols for WSNs

Extensive work has been done on aggregation applications in WSNs. However, security and energy-two major aspects for design of an efficient and robust aggregation algorithm have not attracted adequate attention. Before discussing some of the existing secure aggregation mechanisms, I present a few well-known aggregation schemes for WSNs.

In a framework for flexible aggregation in WSNs has been presented following snapshot aggregation approach without addressing issues like energy efficiency and security in the data aggregation process. A cluster-based algorithm has been proposed in that uses directed diffusion technique to gather a global perspective utilizing only the local nodes in each cluster. The nodes are assigned different level – level 0 being assigned to the nodes lying at the lowest level. The nodes at the higher levels can communicate with the nodes in the same cluster and the cluster head node. This effectively enables localized cluster computation. The nodes at the higher level communicate the local information of the cluster to get a global picture of the network aggregation. In the authors have proposed a mechanism called TAG – a generic data aggregation scheme that involves a language similar to SQL for generating queries in a WSN. In this scheme, the base station (BS) generates a query using the query language, and the sensor nodes send their reply using routes constructed based on a routing tree.

Secure Aggregation Protocol

A secure aggregation (SA) protocol has been proposed that uses the µ TESLA protocol . The protocol is resilient to both intruder devices and single device key compromises. In the proposition, the sensor nodes are organized into a tree where the internal nodes act as the aggregators. However, the protocol is vulnerable if a parent and one of its child nodes are compromised, since due to the delayed disclosure of symmetric keys, the parent node will not be able to immediately verify the authenticity of the data sent by its children nodes. I have presented a secure information aggregation (SIA) framework for sensor networks. The framework consists of three categories of node: a home server, base station and sensor nodes. A base station is a resource-enhanced node which is used as an intermediary between the home server and the sensor nodes, and it is also the candidate to perform the aggregation task. SIA assumes that each sensor has a unique identifier and shares a separate secret cryptographic key with both the home server and the aggregator. The keys enable message authentication and encryption if data confidentiality is required.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Moreover, it further assumes that the home server and the base station can use a mechanism, such as μ TESLA, to broadcast authenticated messages. The proposed solution follows aggregate-commit-prove approach. In the first phase: aggregate- the aggregator collects data from sensors and locally computes the aggregation result using some specific aggregate function. Each sensor shares a key with the aggregator. This allows the aggregator to verify whether the sensor reading is authentic. However, there is a possibility that a sensor may have been compromised and an adversary has captured the key. In the proposed scheme there is no mechanism to detect such an event. In the second phase: commit- the aggregator commits to the collected data. This phase ensures that the aggregator actually uses the data collected from the sensors, and the statement to be verified by the home server about the correctness of computed results is meaningful.

Energy-Efficient Secure Pattern-based Data Aggregation Protocol

I propose an energy-efficient secure pattern-based data aggregation (ESPDA) protocol for wireless sensor networks. ESPDA is applicable for hierarchy-based sensor networks. In ESPDA, a cluster-head first requests sensor nodes to send the corresponding pattern code for the sensed data. If multiple sensor nodes send the same pattern code to the cluster-head, only one of them is permitted to send the data to the cluster-head. ESPDA is secure because it does not require encrypted data to be decrypted by cluster-heads to perform data aggregation.

Secure Hop-by-Hop Data Aggregation Protocol (SDAP)

A secure hop-by-hop data aggregation protocol (SDAP) has been proposed in which a WSN is dynamically partitioned into multiple logical sub-trees of almost equal sizes using a probabilistic approach. In this way, fewer nodes are located under a high-level sensor node, thereby reducing potential security threats on nodes at higher level. Since a compromised node at higher level in a WSN will cause more adverse effect on data aggregation than on a lower-level node, the authors argue that by reducing number of nodes at the higher level in the logical tree, aggregation process becomes more secure.

Data Aggregation And Authentication (DAA) Protocol

A data aggregation and authentication (DAA) protocol is proposed in to integrate false data detection with data aggregation and confidentiality. In this scheme, a monitoring algorithm has been proposed for verifying the integrity of the computed aggregated result by each aggregator node.

Existing System

Data aggregation in intermediate nodes (called aggregator nodes) is an effective approach for optimizing consumption of scarce resources like bandwidth and energy in Wireless Sensor Networks (WSNs). However, in-network processing poses a problem for the privacy of the sensor data since individual data of sensor nodes need to be known to the aggregator node before the aggregation process can be carried out. In applications of WSNs, privacy-preserving data aggregation has become an important requirement due to sensitive nature of the sensor data. Researchers have proposed a number of protocols and schemes for this purpose.I have proposed a protocol - called CPDA – for carrying out additive data aggregation in a privacy-preserving manner for application in WSNs. The scheme has been quite popular and well-known. In spite of the popularity of this protocol, it has been found that the protocol is vulnerable to attack and it is also not energy-efficient.

Proposed System:

Secure And Energy Efficient Data Aggregation With Nasty Aggregator Naming(NAN)

In this segment, I show a safe and vitality proficient information total with frightful aggregator naming (NAN). For effortlessness, I depict our plan for the SUM total capacity. Notwithstanding, our outline helps different other conglomeration capacities, for example, MAX/MIN, MEAN, COUNT, etc. I apply our plan on the total tree demonstrated in Aggregator tree Conglomeration duty: Before depicting the points of

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

interest of the proposed plan, I first present the arrangement of the parcels transmitted amid the accumulation. Every hub has a related parcel to speak to its information that is transmitted to its parent. Such a bundle has the accompanying configuration: ⟨id, tally, esteem, signature⟩ where id is the hub's ID, tally is the quantity of leaves in the sub-tree established at this hub, quality is the accumulation result figured over all the leaves in the sub-tree, and mark is a guarantee processed by the hub utilizing its private The packet for node ui can be inductively expressed as:
⟨uRiR, CRiR, VRiR, SRiR⟩ where SRiR is a cryptographic hash function over the packet value. If uRiR is a leaf node, then CRiR = 1 and VRiR = rRuiR, where rRuiRisthe data collected by node uRiR. If uRiR is an intermediate node havingchild nodes vj (j = 1, 2, . . . , k) with packets ⟨vRjR, CRjR, VRjR, SRjR⟩, then $Ci = \Sigma\ Cj\ k\ \ j=1$, $Vi = \Sigma\ Vj\ k\ j\ =1$ (1) The pair-wise key shared between ui and its parent node is used to encrypt the packet. This encryption in practice provides not only confidentiality but also authentication. Using encryption saves the bandwidth that will otherwise be used for an additional message authentication code.

The proposed secure aggregation algorithm

In the proposed distributed estimation algorithm, a sensor node instead of transmitting a partially aggregated result, maintains and if required, transmits an estimation of the global aggregated result. The global aggregated description in general will be a vector since it represents multi-dimensional parameters sensed by different nodes. A global estimate will thus be a probability density function of the vector that is being estimated. However, in most of the practical situations, due to lack of sufficient information, complex computational requirement or unavailability of sophisticated estimation tools, an estimate is represented as: (estimated value, confidence indication), which in computational terms can be represented as: (average of estimated vector, covariance matrix of estimated vector). For the sake of manipulability with tools of estimation theory, I have chosen to represent estimates in the form of (A, PAA) with A being the mean of the aggregated vector and PAA being the covariance matrix of vector A. For the max aggregation function, vector A becomes a scalar denoting the mean of the estimated max, and PAA becomes simply the variance of A.

In the snapshot aggregation, a node does not have any control on the rate at which it send information to its parents; it has to always follow the rate specified the user application. Moreover, every node has little information about the global parameter, as it has no idea about what is happening beyond its parent. In proposed approach, a node accepts estimations from all of its neighbors, and gradually gains in knowledge about the global information. It helps a node to understand whether its own information is useful to its neighbors. If a node realizes that its estimate could be useful to its neighbors, it transmits the new estimate. Unlike snapshot aggregation where the node transmits its estimate to its parent, in the proposed scheme, the node broadcasts its estimate to all its neighbors. Moreover, there is no need to establish and maintain a hierarchical relationship among the nodes in the network. This makes the algorithm particularly suitable for multiple user, mobile users, faulty nodes and transient network partition situations.

The proposed algorithm has the following steps:

1. Every node has an estimate of the global aggregated value (global estimate) in the form of (mean, covariance matrix). When a node makes a new local measurement, it makes an aggregation of the local observation with its current estimate. This is depicted in the block Data Aggregation 1 in Fig. 5. The node computes the new global estimate and decides whether it should broadcast the new estimate to its neighbors. The decision is based on a threshold value as explained in Section 8.4.

2. When a node receives a global estimate from a neighbor, it first checks whether the newly received estimate differs from its current estimate by more than a pre- defined threshold.
a. If the difference does not exceed the threshold, the node makes an aggregation of the global estimates (its current value and the received value) and computes a new global estimate. This is depicted in the block Data

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Aggregation 2 in Fig. 5. The node then decides whether it should broadcast the new estimate.

b. If the difference exceeds the threshold, the node performs the same function as in step (a). Additionally, it requests its other neighbors to send their values of the global estimate.

c. If the estimates sent by the majority of the neighbors differ from the estimate sent by the first neighbor by a threshold value, then the node is assumed to be compromised. Otherwise, it is assumed to be normal.

3. If a node is identified to be compromised, the global estimate previously sent by it is ignored in the computation of the new global estimate and the node is isolated from the network by a broadcast message in its neighborhood.

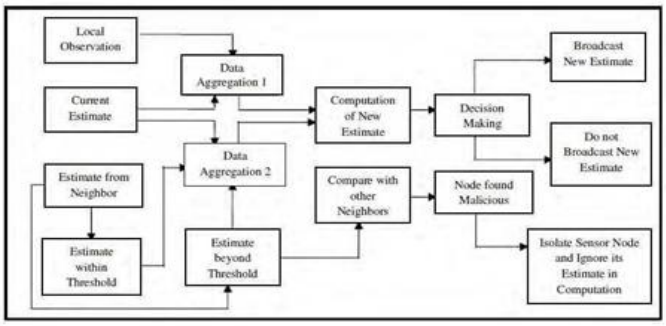


Fig. 5. A Schematic flow diagram of the proposed aggregation algorithm

Aggregation of two global estimates

In Fig. 5, the block Data Aggregation 1 corresponds to this activity. For combining two global estimates to produce a single estimate, covariance intersection (CI) algorithm is used. CI algorithm is particularly suitable for this purpose, since it has the capability of aggregating two estimates without requiring any prior knowledge about their degree of correlation. This is more pertinent to WSNs, as I cannot guarantee statistical independence of observed data in such networks.

Given two estimates (A, PAA) and (B, PBB), the combined estimate (C, PCC) by CI is given by (23) and (24):

$$P_{CC} = (\omega * P_{AA}^{-1} + (1-\omega) P_{BB}^{-1})^{-1} \quad (23)$$

$$C = P_{CC}(\omega * P_{AA}^{-1} * A + (1-\omega) P_{BB}^{-1} * B) \quad (24)$$

Here, P_{AA}, P_{BB}, and P_{CC} represent the covariance matrices associated with the estimates A, B, and C respectively.

The main computational problem with CI is the computation of ω. The value of ω lies between 0 and 1. The optimum value of ω is arrived at when the trace of the determinant of P_{CC} is minimized.

For max aggregation function, covariance matrices are simple scalars. It can be observed from (23) and (24) that in such a case ω can be either 1 or 0. Subsequently, P_{CC} is equal to the minimum of P_{AA} and P_{BB}, and C is equal to either A or B depending on the value of P_{CC}. Even when the estimates are reasonably small-sized vectors, there are efficient algorithms to determine ω.

Aggregation of a local observation with a global estimate

This module corresponds to the block Data Aggregation 2 in Fig. 5. Aggregation of a local observation with a global estimate involves a statistical computation with two probability distributions.

Case 1: Mean of the local observation is greater than the mean of the current global estimate: In case of max aggregation function, if the mean of the local observation is greater than the mean of the current global estimate, the local observation is taken as the new estimate. The distribution of the new estimate is arrived at by multiplying the distribution of the current global estimate by a positive fraction (w_1) and summing it with the distribution of the local observation. The fractional value determines the relative weight assigned to the value of the global estimate. The weight assigned to the local observation being unity.

Case 2: Mean of the local observation is smaller than the mean of the current global estimate: If a node observes that the mean of the local observation is smaller than its current estimate, it combines the two distributions in the same way as in Case 1 above, but this time a higher weight (w_2) is assigned to the distribution having the higher mean (i.e. the current estimate).I observed in this

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

case should be handled more carefully if there is a sharp fall in the value of the global maximum. I follow the same approach as proposed If the previous local measurement does not differ from the global estimate beyond a threshold value, a larger weight is assigned to the local measurement as in Case 1. In this case, it is believed that the specific local measurement is still the global aggregated value.

For computation of the weights w_1 and w_2 in Case 1 and Case 2 respectively. Since all the local measurements and the global estimates are assumed to follow Gaussian distribution, almost all the observations are bounded within the interval $[\mu \pm 3*\sigma]$.

When the mean of the local measurement is larger than the mean of the global estimate, the computation of the weight (w_1) is done as follows. Let us suppose that l(x) and g(x) are the probability distributions for the local measurement and the global estimate respectively. If l(x) and g(x) can take non-zero values in the intervals $[x_1, x_2]$ and $[y_1, y_2]$ respectively, then the weight $w_1(x)$ will be assigned a value of 0 for all $x_1 - 3*$ and $w_1(x)$ will be assigned a value of 1 for all $x_1 - 3*$. Here, x_1 is equal to $\mu 1 - 3*\sigma 1$, where $\mu 1$ and $\sigma 1$ are the mean and the standard deviation of $l(x)$ respectively.

When the mean of the local measurement is smaller than the mean of the global estimate, the computation of the weight w_2 is carried out as follows. The value of $w_2(x)$ is assigned to be 0 for all x $max\{1 - 3*1, 2 - 3*2\}$. $w_2(x)$ is assigned a value of 1 for all x $max\{1 - 3*_1, _2 - 3*_2\}$. Here, y_1 is equal to $2 - 3*2$, where 2 and 2 represent the mean and the standard deviation of $g(x)$ respectively.

In all these computations, it assumed that the resultant distribution after combination of two bounded Gaussian distributions is also a Gaussian distribution. This is done in order to maintain the consistency of the estimates. The mean and the variance of the new Gaussian distribution represent the new estimate and the confidence (or certainty) associated with this new estimate respectively.

Optimization of communication overhead

Optimization of communication overhead is of prime importance in resource constrained and bandwidth-limited WSNs. The block named Decision Making in Fig. 5 is involved in this optimization mechanism of the proposed scheme. This module makes a trade-off between energy requirement and accuracy of the aggregated results.

To reduce the communication overhead, each node in the network communicates its computed estimate only when the estimate can bring a significant change in the estimates of its neighbors. For this purpose, each node stores the most recent value of the estimate it has received from each of its neighbors in a table. Every time a node computes its new estimate, it checks the difference between its newly computed estimate with the estimates of each of its neighbors. If this difference exceeds a pre-set threshold for any of its neighbors, the node broadcasts its newly computed estimate.

The determination of this threshold is crucial as it has a direct impact on the level of accuracy in the global estimate and the energy expenditure in the WSN. A higher overhead due to message broadcast is optimized by maintaining two-hop neighborhood information in each node in the network. This eliminates communication of redundant messages. This is illustrated in the following example.

Suppose that nodes A, B and C are in the neighborhood of each other in a WSN. Let us assume that node A makes a local measurement and this changes its global estimate. After combining this estimate with the other estimates of its neighbors as maintained in its local table, node A decides to broadcast its new estimate. As node A broadcasts its computed global estimate, it is received by both nodes B and C. If this broadcast estimate changes the global estimate of node B too, then it will further broadcast the estimate to node C, as node B is unaware that the broadcast has changed the global estimate of node C also. Thus the same information is propagated in the same set of nodes in the network leading to a high communication overhead in the network.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

To avoid this message overhead, every node in the network maintains its two- hop neighborhood information. When a node receives information from another node, it not only checks the estimate values of its immediate neighbors as maintained in its table but also it does the same for its two-hop neighbors. Thus in the above example, when node B receives information from node A, it does not broadcast as it understands that node C has also received the same information from node A, since node C is also a neighbor of node A. The two-hop neighborhood information can be collected and maintained by using algorithms..

The choice of the threshold value is vital to arrive at an effective trade-off between the energy consumed for computation and the accuracy of the result of aggregation. For a proper estimation of the threshold value, some idea about the degree of dynamism of the physical process being monitored is required. A more dynamic physical process puts a greater load on the estimation algorithm thereby demanding more energy for the same level of accuracy. If the user has no information about the physical process, he can determine the level of accuracy of the aggregation and the amount of energy spent dynamically as the process executes.

Security in aggregation scheme

The security module of the proposed scheme assumes that the sensing results for a set of sensors in the same neighborhood follows a normal distribution. Thus, if a node receives estimates from one (or more) of its neighbors that deviates from its own local estimate by more than three times its standard deviation, then the neighbor node is suspected to have been compromised or failed. In such a scenario, the node that first detected such an anomaly sends a broadcast message to each of its neighbors requesting for the values of their estimates.

If the sensing result of the suspected node deviates significantly (i.e., by more than three times the standard deviation) from the observation of the majority of the neighbor nodes, then the suspected node is detected as malicious. Once a node is identified as malicious, a broadcast message is sent in the neighborhood of the node that detected the malicious node and the suspected node is isolated from the network activities.

However, if the observation of the node does not deviate significantly from the observations made by the majority of its neighbors, the suspected node is assumed to be not malicious. In such a case, the estimate sent by the node is incorporated in the computation of the new estimate and a new global estimate is computed in the neighborhood of the node.

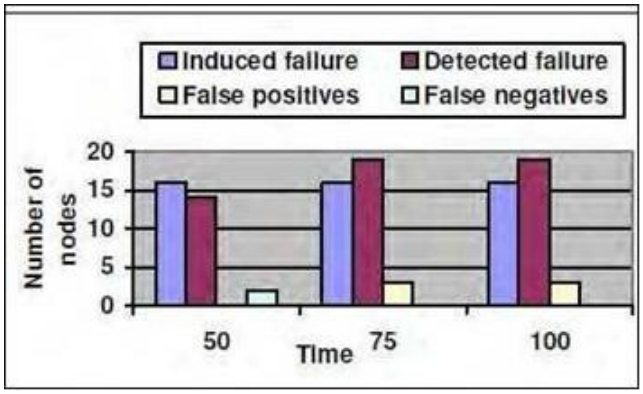
Results

In this section, I describe the simulations that have been performed on the proposed scheme. As the proposed algorithm is an extension of the algorithm.I present here the results that are more relevant to our contribution, i.e., the performance of the security module. The results related to the energy consumption of nodes and aggregation accuracy for different threshold values are presented and therefore these are not within the scope of this work. To evaluate the performance of the security module of the proposed algorithm, two different scenarios are simulated. In the first case, the aggregation algorithm is executed in the nodes without invoking the security module to estimate the energy consumption of the aggregation algorithm. In the second case, the security module is invoked in the nodes and some of the nodes in the network are intentionally compromised. This experiment allows us to estimate the overhead associated with the security module of the algorithm and its detection effectiveness.

Parameter	Value
No. of nodes	160
Simulation time	200 s
Coverage area	120 m * 120 m
Initial energy in each node	5 Joules
MAC protocol	IEEE 802.11
Routing protocol	None
Node distribution	Uniform random
Transmission power of each node	12 mW
Transmission range	15 m
Node capacity	5 buffers
Energy spent in transmission	0.75 W
Energy spent in reception	0.25 mW
Energy spent in sensing	10 mW
Sampling period	0.5 s
Node mobility	Stationary

Table 3. Simulation parameters

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal



It is observed that delivery ratio (ratio of the packets sent to the packets received by the nodes) is not affected by invocation of the security module. This is expected, as the packets are transmitted in the same wireless environment, introduction of the security module should not have any influence on the delivery ratio.

Regarding energy consumption, it is observed that the introduction of the security module has introduced an average increase of 105.4% energy consumption in the nodes in the network. This increase is observed when 20% of the nodes chosen randomly are compromised intentionally when the aggregation algorithm was executing. This increase in energy consumption is due to additional transmission and reception of messages after the security module is invoked.

To evaluate the detection effectiveness of the security scheme, further experiments are conducted. For this purpose, different percentage of nodes in the network is compromised and the detection effectiveness of the security scheme is evaluated. Fig. 6 and Fig. 7 present the results for 10% and 20% compromised node in the network respectively. In these diagrams, the false positives refer to the cases where the security scheme wrongly identifies a sensor node as faulty while it is actually not so. False negatives, on the other hand, are the cases where the detection scheme fails to identify a sensor node which is actually faulty. It is observed that even when there are 20% compromised nodes in the network the scheme has a very high detection rate with very low false positive and false negative rate. The results show that the proposed mechanism is quite effective in detection of failed and compromised nodes in the network.

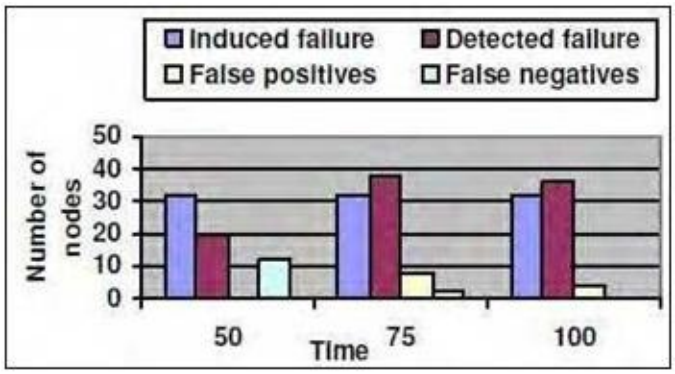


Fig. 7. Detection effectiveness with 20% of the nodes in the network faulty.

Input Design

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy.

Objectives

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.
2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.
3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

Output Design

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
2. Select methods for presenting information.
3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

Future Scope

Future work will focuses on the using new different routing algorithms for routing the data from the source to the sink. Our approach should confront with the difficulties of topology construction, data routing, loss tolerance by including several optimization techniques that further decrease message costs and improve tolerance to failure and loss. In addition to implementing these techniques, I need to rethink some of these techniques to present more efficiency to network changes and external factors which could affect our approach such as node mobility, obstacles and other issues. In addition as future work, I could also extend our simulator to incorporate a 3D tree construction technique.

CONCLUSION

In-network data aggregation is an important technique which saves energy and communication bandwidth and thereby increasing the lifetime of sensor node for data collection in wireless sensor networks. Here I made a comparative assay of communication and computational overhead of the original CPDA to the modified version of less message transmission overheads in the network and computational load on participating sensor nodes.

References

1. J. Sen, "A survey on wireless sensor network security," International Journal of Communication Networks and Information Security (IJCNIS), vol. 1, no. 2, pp. 59-82, August 2009.

2. Mr. Pechetti Murali,"Secure And Data Energy Efficient Data Aggregation In Wireless Sensor Networks" Under The Guidence of Ms. M Neelima And Dr.Y.Venkateswarlu(Prof&HOD),International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-4, July 2015 ISSN: 2395-3470.

3. W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher, "PDA: privacy- preserving data aggregation in wireless sensor networks," Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM'07), pp. 2045-2053, Anchorage, Alaska,USA, May 2007.

4. M. Acharya, J. Girao, and D. Westhohh, "Secure comparison of encrypted data in wireless sensor networks", Proceedings of the 3rd International Symposium on Modelling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WIOPT), pp. 47-53, Washington, DC, USA, 2005.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

5. C. Castelluccia, A. C-F. Chan, E. Mykletun, and G. Tsudik, "Efficient and provably secure aggregation of encrypted data in wireless sensor networks," ACM Transactions on Sensor Networks, vol. 5, no. 3, May 2009.

6. J. Girao, D. Westhoff, and M. Schneider, "CDA: concealed data aggregation for reverse multicast traffic in wireless sensor networks," Proceedings of the 40th IEEE Conference on Communications (IEEE ICC'05), vol. 5, pp. 3044– 3049, Seoul, Korea, May 2005.

7. D. Westhoff, J. Girao, and M. Acharya, "Concealed data aggregation for reverse multicast traffic in sensor networks: encryption, key distribution, and routing adaptation," IEEE Transactions on Mobile Computing, vol. 5, no. 10, pp. 1417-1431, October 2006.

8. F. Armknecht, D. Westhoff, J. Girao, and A. Hessler, "A lifetimeoptimized end-to-end encryption scheme for sensor networks allowing in-network processing," Computer Communications, vol. 31, no. 4, pp. 734-749, March 2008.

9. S. Peter, D. Westhoff, and C. Castelluccia, "A survey on the encryption of convergecast traffic with in-network processing," IEEE Transactions on Dependable and Secure Computing, vol. 7, no. 1, pp. 20–34, February 2010.

10. L. Hu and D. Evans, "Secure aggregation for wireless networks," Proceedings of the Symposium on Applications and the Internet Workshops (SAINT'03), pp. 384-391, Orlando, Florida, USA, January 2003.

11. H. Cam, S. Ozdemir, P. Nair, D. Muthuavinashiappan, and H. O. Sanli, "Energy-efficient secure pattern based data aggregation for wireless sensor networks," Computer Communications, vol. 29, no. 4, pp. 446-455, February 2006.

12. K. Wu, D. Dreef, B. Sun, and Y. Xiao, "Secure data aggregation without persistent cryptographic operations in wireless sensor networks," Ad Hoc Networks, vol. 5, no. 1, pp. 100–111, January 2007.

13. J. Sen, M. G. Chandra, P. Balamuralidhar, S. G. Harihara, and H. Reddy, "A distributed protocol for detection of packet dropping attack in mobile ad hoc networks", in Proceedings of the IEEE International Conference on Telecommunications and Malaysian International Conference on Communications (ICT-MICC'07), , Penang, Malaysia, May 2007.

14. S. Ozdemir, "Secure and reliable data aggregation for wireless sensor networks," in Proceedings of the 4th International Conference on Ubiquitous Computing Systems (UCS'07). Lecture Notes in Computer Science (LNCS), Ichikawa et al. (eds.), vol. 4836, pp. 102-109, Springer-Verlag Berlin, Heidelberg, Germany 2007.

15. J. Sen, "A distributed trust and reputation framework for mobile ad hoc networks," in Proceedings of the 1st International Conference on Network Security and its Applications (CNSA'10), Chennai, India, July 2010. Recent Trends in Network Security and its Applications, Meghanathan et al. (eds.), pp. 528–537, Communications in Computer and Information Science (CCIS), Springer-Verlag, Heidelberg, Germany, July 2010.

16. J. Sen, "A trust-based detection algorithm of selfish packet dropping nodes in a peer-to-peer wireless mesh networks,". In Proceedings of the 1st International Conference on Network Security and its Applications (CNSA'10), Chennai, India, July 2010. Recent Trends in Network Security and its Applications, Meghanathan et al. (eds.), pp. 538–547, Communications in Computer and Information Science (CCIS), Springer- Verlag, Heidelberg, Germany, July 2010.

17. J. Sen, "Reputation- and trust-based systems for wireless self-organizing networks," pp. 91-122, Security of Self-Organizing Networks: MANET, WSN, WMN, VANET, A-S. K. Pathan (ed.), Aurbach Publications, CRC Press, USA, December 2010.

18. J. Sen, "A robust and secure aggregation protocol for wireless sensor networks," in Proceedings of the 6th International Symposium on Electronic Design, Test and

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Applications (DELTA'11), pp. 222-227, Queenstown, New Zealand, January, 2011.

19. C. Fontaine and F. Galand, "A survey of homomorphic encryption for nonspecialists," EURASIP Journal on Information Security, vol. 2007, article id 13801, January 2007.

20. D. Chaum, "The dining cryptographers problem: unconditional sender and recipient untraceability," Journal of Cryptography, vol. 1, no. 1, pp. 65-75, 1988.

21. L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in Proceedings of the 9th ACM Conference on Computing. and Communication Security (CCS'02), pp. 41- 47, Washington DC, USA, November 2002.

22. S. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong, "TAG: a tiny aggregation service for ad-hoc sensor networks," in Proceedings. Of the 5th Symposium on Operating Systems Design and Implementation (OSDI'02), pp. 131-146, Boston, Massachusetts, USA, December 2002.