ISSN 2348-375X

Unique Journal of Engineering and Advanced Sciences

Available online: www.ujconline.net

Research Article

A REFINEMENT FOR SECURE DATAGATHERING IN WIRELESS SENSOR NETWORKS

Gayathri J[1*], Manikandaprabu N[2], Dhusara P[3], Anguraj S[4]

[1] PG Scholar, Department of CSE, Sri Guru Institute of Technology, TN
[2]Lecturer, Department of ECE & Senthur Polytechnic College, TN
[3]PG Scholar, Department of ECE, Sri Guru Institute of Technology, TN
[4] PG Scholar, Department of ECE, PPG Institute of Technology, TN

Received: 26-12-2013; Revised: 25-01-2014; Accepted: 21-02-2014

*Corresponding Author**: J. Gayathri,** PG Scholar & Sri Guru Institute of Technology Email:gayathrij19@gmail.com.

ABSTRACT

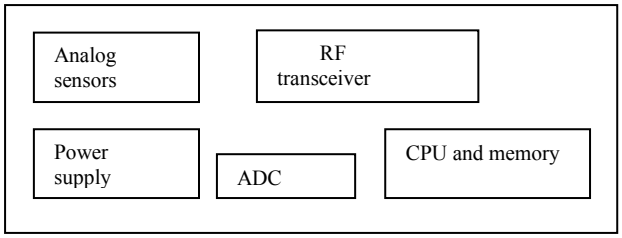
In this paper, Intend to new data gathering security in the Wireless Sensor Network (WSN).WSNs are spatially distributed in self directed sensor nodes without relay. In this paper may be mobile self directed or a transport equipped with a powerful battery, transceiver and memory. Working like a mobile support place and gathering data while moving through the area.In this paper ,we purpose new data gathering scheme for wide area wireless sensor networks, mainly gathering the data from sensors using single or multiple M-Investor are used, A Mobile Data Investor for simply called as M-Investor. only one m- Investor used to gather the data from sensor node and upload the data into data sink. One M-Investor moving gather the data from the entire network of each and every sensor nodes to the data sink because raise distance/time constraints. We think utilizing Multiple Investers and intend a data-gathering algorithm where multiple M- Investors moving through a number of smaller subtours parallel to satisfy the distance/time constraints. Dynamically moving way to non visible link between partioned small networks and each of them moving through a number of smaller subtours of the entire network to gathering a data. . It can be used in both joined and disjoined networks..In enhance ,sensor node may collect the sensitive data because to provide the security. Make sure of security of contact and access control in Wireless Sensor Networks(WSNs) is of greatest worth. Simulation results demonstrate that the intend data-gathering algorithm can greatly shorten the moving distance of the Investor compared with the *shortest path* algorithm and is close to the optimal algorithm for small networks and The results demonstrate that MoteSec-Aware consumes much less power, but get higher security than some state-of-the-art methods.

Keywords: Shortest path algorithm, data-gathering, M-Investor, Mobile Data Investor, security, Wireless Sensor Networks (WSNs).

INTRODUCTION

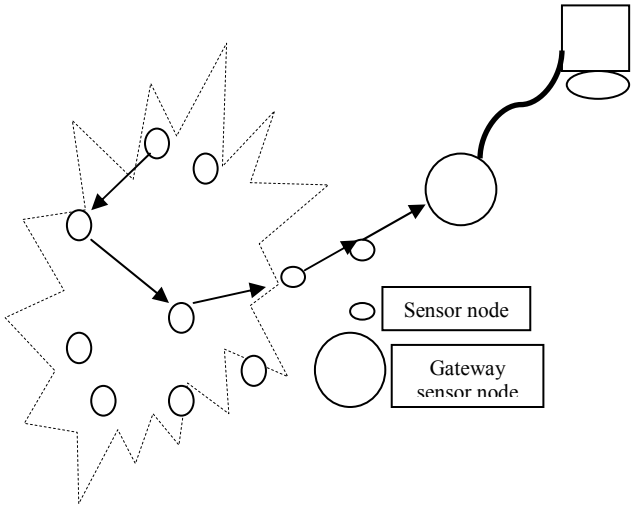
Wireless networks of graceful sensors have develop into sensible for several applications because of hi-tech progress in chip power resourceful wireless connections, and reduced power budgets for computational devices, as well as the development of novel sensing materials. Sensor is a one of the convertor. A basic wireless sensor node divided into some general components, also the CPU, and memory, the sensor node has, of course, a number of analog sensors. These sensor outputs must be converted to digital data that can be processed by the CPU. This transformation is performed by the analog-to-digital converter(ADC). Batteries could provide the wireless sensor node with power as indicated by the power supply component. Although other wireless contact mechanisms are potential, the majority of wireless sensor nodes use radio frequency (RF) transmissions, so the final part shown in the sensor node is the RF transceiver. The whole sensor node is summarize in the suitable packaging for the background in which the sensor node will perform. In the near future, it is logical to expect that knowledge has higher to the point where rate-efficient implementations of these sensor nodes permit for wide installments of big level size of WSNs. WSNs to support a specific application, several tasks need to be allowed, such as neighbor discovery, sensor data processing, data aggregation, storage, and caching, medium access control, battlefield surveillance, habitat monitoring, etc. wireless sensors to attain their designed purpose of sensing, watching and gathering information.

While the sensor nodes are prepared with small, often static, power saver with limited power faculty, it is required that the network be rate-efficient in order to maximize its duration of a new data-gathering mechanism for of big level size wireless sensor networks by starting mobility into the network.



Generic wireless sensor node

Wireless sensor network is a set of nodes structured in a network. Single node consists of one or more microregulator, chips, storage and a RF transmitter and receiver, a power source such as power saver and staying place a variety of sensors and Transducers. The nodes connection without wireless and regularly self-organize after being deployed in an ad hoc fashion. Sensor nodes are normally spread into a large-scale sensing field without a prearranged communications. Before watching the background, sensor nodes should be able to learn nearby nodes and arrange themselves into a network.



Sensor Network

RELATED WORK

In[1],Most of the vigor of a sensor is inspired on perfoming two important responsibilities: sensing data in the field and after that data to forward the data sink. Power cabability spend on sensing is reasonably steady because it only depends on the sampling cost and but independ on the place of that sensors. Another responsibility of the data-gathering plan is very important aspect that determines network duration. A Mobile Data Investor is completely suitable for such applications. Mobile Data Investor serves as a mobile "data transporter"that moves through every community and association all separated smallnetworks jointly.The moving path of the mobile data investor perform as virtual link between sepearated small networks.In[3], a stochastic compressive data-collection protocol for mobile WSNs, named SMITE, was presented. SMITE consists of three parts: 1) random collector election; 2) stochastic direct transmission from common nodes to investors when common nodes are in the investors transmission range; and 3) angle transmission from investors to the mobile sink when investors gathered enough data using a predictive method. In[12],Data gathering in wireless sensor networks by servicing mobile investors that gather the data by way of small value of communications. Data collection latency can be efficient reduced by presenting nearly collection by way of multi way broadcasting and then data to forwarding the packets from relay sensors to the mobile investors. A Selection-based mobile collection method and create it into an max-min problem, named bounded relay hop mobile data collection (BRH-MDC). Specifically, a inside set of sensors will be chosed as polling points(selection points) that temporary storage nearly gathered data and forward the data to the mobile investor when it reach that area.

In this paper, we consider applications , Generally sensing to gathering data at low rate but not postponement that data can be placed into data packets within fixed lenth. WSNs are spatially distributed in self directed sensor nodes without relay. Mobile Data Investor used to gather data from sensors.Specifically,a Mobile Data Investor may be mobile self directed or a transport equipped with a powerful battery, transceiver and memory. ,A Mobile Data Investor for simply called as M-Investor, Used to gather the data from sensor node and upload the data into data sink.Since sensor nodes may collect confidential information because to provide the security.most of the real world applications, as well as environment monitoring,smart home require data transmission via network and data storage in node of large memory.In the main issues of secure network protocol and data access control in WSNs in steps to reduce data escape to the unauthorized person.

Here, we briefly summarize some related work on data-gathering mechanisms in WSNs. In[1],only one m- Investor used to gather the data from sensor node and upload the data into data sink. One M-Investor moving gather the data from the entire network of each and every sensor nodes to the data sink because raise distance/time constraints.then this m-investor gather data is confidential but may affect internal and external attack,the third person does not control any suitable nodes in that network.

To overcome this problem, some works in the literature have introduced a hierarchy to the network[4-8]. Kun *et al.*'s method[9] is included of three phase: network admission control, network access control, and network access maintenance. . In truth, MoteSec-Aware provides (1) a secure network protocol to allow data convey in an encrypted format without link and (2) a sortout ability to authorize or deny data access based upon a protocol, which are often used to protect the data from unauthorized access while permitting reasonable communications to pass.

In[10], A forming SNEP means *Secure Network Encryption Protocol,* providing basic security primitives data privacy and secrecy,data authenticationwith two parties, and data brightness, with low overhead. A mainly hard problem is to provide efficient broadcast verification, which is an significant method for sensor networks. SNEP achieves even semantic security, prevents hackers from gather the data content from the encrypted data. Finally the same Simple and efficient protocol also gives us data authentication, replay protection,

and weak data brightness.Data privacy and secrecy is most important basic security primitives and it is used in security of set of rules.A easy form of confidentiality can be achieved through encryption, but clear encryption is not enough . Another important security law is semantic security, which make sure that an hacker has no information about the original data, even if it doing multiple times to encryptions of the same data.

In[13],A Constrained Function based message Authentication (CFA) method for wireless sensor networks which gather to all the resource of the so-called sensor verification principle, while more over existing method only gain fractional supplies. In specifically , to the greatest of our skill, CFA is the first verification method supporting enpath reducing with only a each packet overflow. The node ID is artificial, most important to hardware dependency and hence restricted applications. As a final point, it is precious of mentioning that the proposed CFA method attaining stable communication overflow. In specifically, only one each number representing data authentication code is adequate, while the packet lenth depending on security stage, will be long. It must be noted that data length is very important for some WSN locating with limitation on packet lenth. since data authentication signs can always sum up into a one packet, such unsecurity can be avoid.

Our main work of this paper can be summarized as follows.

1) We intend new data-gathering mechanisms for huge size wide area Sensor networks when one or more M-investors are used.

2) We intend a spanning tree covering algorithm for the Only one M-investors task.

3) We too believe using several M-investors and intend a data-gathering algorithm where several M-investors moving through a number of smaller sub tours parallel to satisfy the distance/time constraints. Gathering data is very confidential one because to provide security.

4)we intend and apply motesec-aware, which is the sensor network security structure build on the network level that view on data admission manage and secure network set of rules concurrently.

5) MoteSec-Aware accomplish lesser power utilization throughout during contact and gratifies a higher security without adding some extra data (*e.g.*, initialization vector) into packets.

In a multi bound standardized network, in our method, M-investors and sensors function in a master –slaves type, and sensors don't want to over listen to the canal every time to relay packets from their nearly. Once an M-investor travel to a polling point, it can convey a toot to awaken for combination of the transmitter and receiver of the closerby sensors, collect data from sensors, and place sensors into lie-down once more. We believe that single sensor is prepared with a reactive RFID tool [32], which make active for combination of the transmitter and receiver of the sensor by transferring an disrupt signal to the microsupervisor, once it accepts the RFID call from the M-investor. The merit of reactive RFID tool is that they don't want energy from sensor power savers and can find energy from the outer RF signal.

TOUR PLANNING

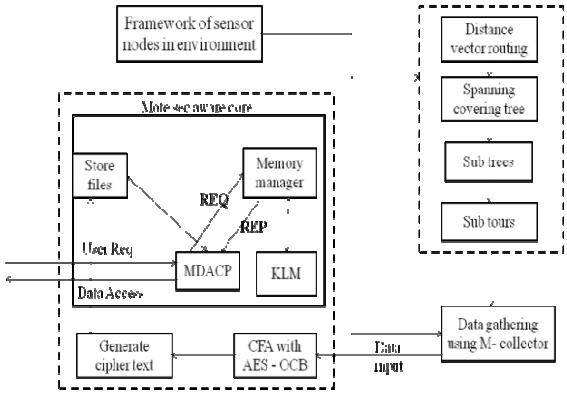
Wireless Sensor Network(WSN) consist of both static and dynamic "nodes"or "mote". Each node consist of a "mote", each such sensor network node has typically several parts a radio transmitter and receiver, microregulator, power source, ADC.A group of mote distributed in a space forms as a WSN.WSN are used to monitor an environmental activities. Each mote gather the data and send to base station. Limited by a range and act as tranceiver. A Mobile Data Investor for simply called as M-Investor. only one m- Investor used to gather the data from sensor node and upload the data into data sink.

In[1], In this paper, we seeing about Data gathering problem in which the M-Investors traverse the transmission range of each and every static sensors ,such that sensing data can be gathered by one hop communication without relay. Before normally describe the data gathering problem, we begin define few important terms are used. While an M-Investor traverse ,it can census nearby sensors one after another to gather data. ahead getting the polling message. easily a sensor upload the data to the m-investor straightforward without relay. M-investor select the sensors as *polling point*. When m-investor traverse to a polling point, it select close by sensors with at the same transmission range of as sensors, that sensors getting polling messages can upload packets to the M-investor in each hop. We define the *neighbor set* of a edge in the level as the group of sensors that can upload data to the M- investor straightforward without relay, if the M-investor selects sensors at this edge. In further terms, the combination of neighbor sets of every polling points should envelop every sensors. Thus, it is only likely to test a fixed digit of points and their parallel neighbor sets in the level, and we should select polling points from this fixed group of points, as the *candidate polling point set*. If the link plan of sensors can be received since the neighbor set of this point is previously known. To receive the candidate polling points without the information on the link plan, after that sensors are installed, many of M-investors require to discover the whole sensing area. While discovering only one M-investor can transmit "Hello" messages at regular intervals with the same transmission range of as sensors. Only one sensor that can decipher the "Hello" message properly response with an "ACK" message to warn the M-Investor where it is. ahead getting the "ACK" message from the sensor, the M-investor characters its present site as a candidate polling point and adds the ID of the sensor into the neighbor set of this candidate polling point. Thus, every wireless links between sensors and the M-investor at the candidate polling points are checked in forward and toward the back route.

SYSTEM ARCHITECTURE

Here the figure consisted of various node attached to servers such that server monitoring operation take place. For each node server calculates hop sequence .If any hacker node is found means it will inform to all nodes which is connected with leader node. This technique is very effective in diminishing the effects of a secure attack.Deploy the framework of sensor nodes in environment for some fixed parameter such as network size, radio range, routing protocol with application. Then Adhoc Ondemand Network Distance

Vector Routing protocol is mainly used for find the edges and vertices of the node between establish the shortest path without relay. To reduce the distance and time consuming to gather data. Spanning covering tree consist of covering all the sensor nodes of polling points, sub tree is a subset of polling points. M-collector traverse the sub tree is known as sub tour. M-collector starts the data gathering tour periodically from the static data sink traverse entire sensor network.



DATA GATHERING USING MULTIPLE M-INVESTORS

One hop data gathering, Only one m-investor traverse to the entire network,thats each and every location of sensors must visit at stable speed and set of already before fixed location of data investing in each sensor.one m-investor is not enough for wide area sensor netwok then time taken also very high and temporary memory is also overflow.To overcome this problem mainly used multiple M-investors,

One of them traverse to smallest sub tour of the whole network to gather the data,that data is very confidential one so to give security in the gathering data packets.

A spanning tree of that graph is a subgraph that is a tree and connects all the vertices together. A single graph can have many different spanning trees. I can also allot a weight to each edge, which is a number representing how unfavorable it is, and use this to allot a weight to a spanning tree by computing the sum of the weights of the edges in that spanning tree. a spanning tree with weight less than or equal to the weight of all other spanning tree. More commonly, any undirected graph (not necessarily connected) has a minimum spanning forest, which is a union of minimum spanning trees for its connected components. The basic idea behind in proposed greedy algorithm is to choose a subset of points from the candidate polling point set, every of which corresponds to a neighbor set of sensors. At each step of the algorithm, a neighbor set of sensors can be enclosed when its corresponding candidate polling point is select as a polling point in the data-gathering tour. The algorithm will conclude after every sensors are enclosed. The algorithm tries to cover each uncovered neighbor set of sensors with the minimum average cost at each stage.

ALGORITHM 1: SPANNING TREE COVERING

Create an empty set P_{curr}
Create a set U_{curr} containing all sensors
Create a set L containing all candidate polling points
While Ucurr ≠ Φ
Find a polling point lЄL,which minimizes $\alpha = \frac{cost\{nb(l)\}}{|nb(l) \cap Ucurr'}$ cover sensor in nb(l)
Add the corresponding polling point of nb(l) into pcurr
Remove the corresponding polling point of nb(l) from L
Remove sensors in nb(l) from Ucurr.
End while
Find an approximate shortest tour on polling point in Pcurr

In[1], the algorithm can be described as follows. Let Pcurr contain all polling points, L be the set of all candidate polling points, and Ucurr contain the set of remaining uncovered sensors at each stage of the algorithm. First, start with an empty set Pcurr. For each candidate polling points l in L, let nb(l) denote the neighbor set of l. Recall that each neighbor set corresponds to a candidate polling point and contains all the sensors that can be polled by the M-collector at this candidate polling point. The distance between two neighbor sets is defined as the distance between their corresponding candidate polling points. Let cost{nb(l)} be the cost of an uncovered neighbor set nb(l), which is equal to the shortest distance between nb(l) and any covered neighbor set.

Let α = cost{nb(l)}/|nb(l)_Ucurr|, which denotes the average cost to cover all uncovered sensors in nb(l).While there are remaining uncovered elements in Ucurr, choose the uncovered neighbor set nb(l) with the minimum α value, add the corresponding candidate polling point l of nb(l) into Pcurr, and remove the corresponding covered sensors from Ucurr. The algorithm terminates when all nodes are covered. Finally, Pcurr contains all polling points in the data-gathering tour. After obtaining all the polling points, the data-gathering tour can be easily obtained by running any approximate algorithm for the TSP. It is interesting to note that in a special case of the SHDGP, when each neighbor set contains only one sensor and no two neighbor sets contain the same sensor,Greedy algorithm is exactly the same as Prim's algorithm for the minimum spanning tree problem, since the M-collector has to visit every candidate polling point to cover all sensors. Thus, the name of greedy algorithm the spanning tree covering algorithm.

IMPLEMENTING DATA GATHERING ALGORITHM

In[1],The data-gathering algorithm with multiple M-collectors can be demonstrated as follows. First, find the polling point set P by running the spanning tree covering algorithm in 1. Then, find the minimum spanning tree T(V,E) on polling points. Refer to the minimum spanning tree on polling points as the spanning covering tree.

ALGORITHM 2: DATA GATHERING

Find the polling point set P
Find the spanning covering tree T on all polling point in P
For each vertex v in T, calculate the weight value weight(v)
While T≠Φ
Find the deepest leaf vertex u in T
Let the root of the sub tree t, Root (t) = u
While weight(Parent (Root(t))) $\leq \frac{Lmax}{2}$
Root (t) = Parent (Root(t))
End while

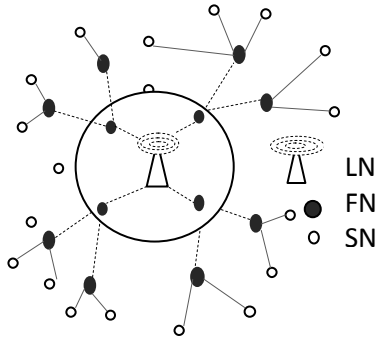
Add all the child vertices of Root(t) and edges connecting them into t and remove t from T
Update weight value of each remaining vertex in T
End while
Let Lmax be the upper bound on the length of any sub tour, which guarantees the data to be collected before sensors run out of storage. Let t(v) denote the sub tree of T, which is rooted at vertex v and consists of all child vertices of v and edges connecting them in T. Let Parent{v} be the parent vertex of v in T. Let Weight{v} represent the sum of all link costs in the sub tree t(v) rooted at v. Repeatedly remove sub trees from T until no vertex is left in T. To build a sub tree t in each loop, start from the deepest leaf vertex of the remaining T, and let it be the root Root(t) of the sub tree t. Check the weight of Parent(Root(t)), and let Root(t) = Parent(Root(t)) if Weight(Parent(Root(t))) ≤ Lmax/2. Otherwise, add all child vertices of Root(t) and edges connecting them in T into t and remove t from T. Here, Weight(Parent(Root(t))) also denotes the total edge length of sub tree t.
After removing the sub tree, upgrade the weight value of each vertex in the remaining T. The algorithm terminates when T is empty. Then T is decomposed into a set of sub trees. The total length of any sub tree t, which is denoted by Lt, is no more than Lmax/2. Finally, the sub tour on polling points of each sub tree can be determined by running the approximation algorithm for the TSP. Let Lt apx be the length of the approximated sub tour on points in sub tree t. In the 2-approximation algorithm for the TSP, the approximated tour is obtained duplicating all edges of the minimum spanning tree and then finding an Eulerian circle in it. Hence, Lt apx is no more than two times the length of the minimum spanning sub tree t Lt, that is, Lt apx ≤ 2 × Lt. As discussed earlier, Lt is bounded by Lmax/2. Thus, I have Lt apx ≤ 2 × Lt ≤ Lmax, which means that the length of any sub tour obtained by the data-gathering algorithm with multiple M-collectors is no more than the upper bound on the length of a sub tour Lmax.

OVERVIEW OF SYSTEM PROCESS AND FUNCTION

We intend Motesec-conscious,a safe network-level protocol for wireless sensor network. More purposely, we support our plan on the existing security primitive, AES, which has been shown to be the most appropriate chunk cipher for the WSNs below thought[11-15].Here a Virtual Counter Manager (VCM) with synchronized incremental counters and discover the Key-Lock Matching (KLM) technique[12] to, respectively, oppose the replay/jamming attacks and obtain memory data access control. In other words, as sensors in the network, mainly those with restricted resources, may affect from DoS attacks, our prior work, called Constrained Function based Authentication (CFA)[13], is worked with suitable alteration to oppose DoS attacks.
Denoting the execution process of CFA in the AES with Offset Codebook Mode(OCB)mode_as AES_OCFA. In our implementation of AES-OCFA is the method planned to get the objective of secure network protocol. In other words Memory Data Access Control Policy (MDACP) is offered to get the objective of data access control. To protect besides unauthorized clients in accessing data, we consider the Key-Lock Matching (KLM) technique[14] to define access privileges in single node because of its feature in requiring low working out overflow In KLM, all user is related with a key (*e.g.*, a prime number) and all folder is related with a lock value. For all folder, there are several equivalent locks, which can be extracted from prime factorization. Through easily work out on the origin of keys and locks, protected memory data can be accessed. Here, data access control is planned completely for function nodes. Note that as the earlier techniques[16-20] were not planned for two-layer networks, which permit header node or mobile node to query data from beginning to end an on-demand communication link to some function nodes, and did not assign the memory sector to usefulness data, appliances, *etc.*, they cannot straightly relate KLM for access control.

MOTESEC-CONSCIOUS NETWORK TOPOLOGY FOR MULTITIER ACCESS

Their association is demonstrated in Fig.1. In our sensor Motesec-conscious network topology divided into three kind of nodes There are leader node (LN), function node (FN), and sensor node (SN), They are separated along with their required hardware resources (remaining energy, memory size, *etc*.) [14].
The network area is divided into corporal clusters, one of which holds a FN in indict of SNs in that cluster.



Motesec-conscious network topology

Depending on real applications, clusters may partly cover such that SNs in the partly covering area are combined with several FNs. In one cluster, SNs are in chargeable for collecting sensed data, while FNs cumulative the data from SNs; send instructions to SNs; maintain function data, appliances, *etc*. in internal memory; and onward the acknowledged data to their higher stage nodes (*i.e.*, LNs, FNs). The LN is a network administrator with plentiful resources that can query data by an on-demand wireless connection linked to all FNs. To avoid storage pour out of FNs, the LN can also be regularly transmit to gather data and clear the storage of FNs.
The opponent may establish both outer and inner attacks. In outer attacks, the opponent does not manage any suitable nodes in the network. Instead, the opponent may effort to spy for sensitive information, insert fake messages, repeat before interrupted messages, and reproduce valid sensor nodes. Moreover, we assume that the opponent can squash the contact between two nodes by transmitting signals that interrupt packet function at the receiver. The opponent may also initiate DoS attacks by, for example, fake data insertion or path-based DoS (PDoS) to reduce the force of FNs. As for

inner attacks, we do not believe that the FN will be absorbed. Instead, we believe that the opponent may effort to study the data stored in FNs' memories by, for instance, make use of an unauthorized node to read main data from FNs randomly.

In view of these vulnerabilities, the serious security necessities that want to be fulfilled are shortened as follows.

• **Data Confidentiality:** This is the fundamental property of a secure communication protocol in that data should be Kept secret from unauthorized reading.

• **Replay and Jamming Detection:** Communication data should be make sured to be current and verified that an opponent does not repeat or squash data.

• **Data Authentication:** It is required to avoid an opponent from spoofing packets. In common, a Message Authentication Code (MAC) is used for every packet to verify whether it really invents from another valid node or is altered during transmission.

• **DoS-Resilience:** The DoS attacks, objective to reduce energies, must be opposed in specifically for resource partial sensor nodes.

• **Data Access:** The opponent should be detected and prevented from accessing data stored on nodes.

PROPOSED METHOD: MOTESEC- CONSCIOUS

we explain the planned AES-OCFA and MDACP approaches for providing defense against external

network messages and inner memory data escape, correspondingly. More particularly, included in AES-OCFA are two procedures for justifying DoS and detecting replay/jamming attacks. Basically, in order to deal with DoS, our before proposed method Constrained Function-based Authentication (CFA) scheme [13] has been correctly modified and incorporated with the AES in OCB mode. Note that AES in OCB mode creates a ciphertext that concurrently provides data privacy and accuracy. In addition, CFA with AES in OCB mode is more well-organized than CFA with AES in CBC-MAC mode since the OCB mode is about two times faster than the CBC-MAC mode. Therefore, the modification give confidence our method to be more powerful.

SECURITY VERSUS DOS ATTACK AND REPLAY AND JAMMING DETECTION

The DoS attacks therefore fake data insertion attack and path based denial of service (PDoS) attack can weaken restricted energies of FNs and maybe black out a section of the monitored region. In sort to deal with DoS attacks, verification is a necessary security mechanism for preventing the communications in the network from DoS attacks. There have been many verification schemes proposed for wireless sensor networks. However, they are not as well-organized in energy consumption as the CFA scheme that we proposed in [13]. In particular, CFA is the first authentication scheme following on the way filtering with only a one packet overhead.

COUNTER SYNCHRONIZATION

At the start, all nodes boot up with the equal counter value. When the network runs for a period of time, the counters of nodes may lose synchronization. Recent advances in secure sensor network time synchronization [20] enable pairwise time synchronization with error of mere μs. Transmission delay between neighboring nodes are on the order of ms. Thus, we launch VCM to synchronize counter value based on Secure Pairwise Synchronization (SPS) protocol [20]. Note that the protocol is modified to conform to the security properties addressed in MoteSec-Aware and the resultant pairwise counter synchronization (PCS) protocol is depicted in Algorithm 4.

MDACP ALGORITHM

1 Set $rij = 0$ and $Temp = Lj$.
2 Calculate $Q = Temp/Ki$. If Q is an integer, set $rij = rij + 1$, $Temp = Q$, repeat this step until Q is not an integer or $rij = rmax$, where $rmax$ is the maximum of access right.
3 Output access right rij .
4 If $rij=Yij$, then execute designate tasks and retrieve corresponding files from the memory; else reject the request.

MEMORY DATA ACCESS CONTROL POLICY (MDACP)

In[2], Let m be the number of users and n be the number of files. We assign a key (Ki, $1 \le i \le m$) to each user and a lock (Lj, $1 \le j \le n$) to each file. Let Ki be a prime number and [rij]m□n be an access right matrix. An example of access right matrix is shown in Fig. 3, where the digit in an entry indicates an access right rij , which defines the right of user Ui in accessing the file Fj . Lj is then computed by $Lj = \_m\ i$=1 $Krij\ i$. To figure out access rights rij 's of users to files, a function f of key Ki and lock Lj is used. Mathematically, $f(Ki, Lj) = rij$. If a user (Ui) asks to access a file (Fj), whether or not the user is legitimate will be verified. The procedure of MDACP is depicted in Algorithm 5, which is used as $f(Ki, Lj)$ to figure out access rights rij 's from keys and locks. As shown in Algorithm 5, the overhead is dependent on the lock values instead of the number of deployed sensor nodes. Thus, MDACP is efficient for a large-scale sensor network.

PCS ALGORITHM

1 A($C1$)→($C2$)B: synchronization packet_*Header, A,B,EKA,B,IV* (*sync*), *MACA*(*B, sync*)_;
2 B($C3$)→($C4$)A: acknowledgement packet_*Header, B,A,EKB,A,IV* ($C2||C3||ack$),*MACB*(*A,* $C2||C3||ack$)_;
3 Calculate counter delay $Cd = (C2-C1)+(C4-C3)2$;
4 if $Cd \le \delta$ **then**
5 Counter offset $\Delta = (C2-C1)-(C4-C3)2$;
6 Node A updates its counter ($C\alpha$): $C\alpha = C\alpha + \Delta$;
7 else
8 The jamming attack is detected and the received packet is dropped.
9 end

PAIRWISE COUNTER SYNCHRONIZATION (PCS)

In[2],node A sends a synchronization packet to B at clock $C1$ and node B receives this packet at $C2$ (Step 1). At clock $C3$, then, B sends back an acknowledgement packet (Step 2). This packet contains the values of $C2$ and $C3$. When node A receives the packet at $C4$, it can now calculate the end-to-end counter delay, Cd (Step 3). In PCS,a jamming attack is detected through a comparison (Steps 4-9) of Cd with δ.In the proposed PCS algorithm (Algorithm 4), message integrity and authenticity are ensured through the use of *MAC*, and of a KA,B (= KB,A) that is shared between A and B (Steps 2 and 4).

This prevents external attackers from successfully modifying any values in the synchronization process. Furthermore, the adversary cannot impersonate node *B* as it does not know the secret key *KA,B*. Replay attacks are avoided by using an IV during the handshake.

CONCLUSION

In this paper, we proposed a mobile data-gathering method for large-scale sensor networks. We introduced a mobile data investor, called an M- investor, which works like a mobile base location in the network. we purpose new data gathering scheme for wide area wireless sensor networks,mainly gathering the data from sensors using multiple M-Investor. One M-Investor moving gather the data from the entire network of each and every sensor nodes to the data sink because raise distance/time constraints.We think utilizing Multiple Investers and intend a data-gathering algorithm where multiple M- Investors moving through a number of smaller subtours parallel to satisfy the distance/time constraints. Dynamically moving way to non visible link between partioned small networks and each of them moving through a number of smaller subtours of the entire network to gathering a data.Our method, MoteSec-conscious, is proposed and implemented for TinyOS on the TelosB platform. MoteSec-conscious is an efficient network layer security system and is the completely implemented security mechanism that provides security for both inside memory data and outside network message. MoteSec-conscious is clever to attain the target of much less energy consumption and higher security than prior works.

REFERENCES

1. Ming Ma, Yuanyuan Yang, Fellow, IEEE, Miao Zhao. Tour Planning for Mobile Data-Gathering Mechanisms in Wireless Sensor Networks IEEE Transactions on Vehicular Technology. 2013; 62(4).
2. Yao-Tung Tsou, Chun-Shien Lu, Member, IEEE, Sy-Yen Kuo, Fellow, IEEE MoteSec-Aware: A Practical Secure Mechanism for Wireless Sensor Networks.
3. Guo L, Beyah R, Li Y. SMITE: A stochastic compressive data collection protocol for mobile wireless sensor networks, in Proc. IEEE INFOCOM. 2011; 1611.
4. Heinzelman WR, Chandrakasan A, Balakrishnan H. Energyefficient communication protocols for wireless microsensor networks," in Proc. HICSS, Maui, HI. 2000; 1.
5. Younis O, Fahmy S. Distributed clustering in ad-hoc sensor networks:A hybrid, energy-efficient approach, in Proc. IEEE INFOCOM,Hong Kong, China. 2004; 629.
6. Amis AD, Prakash R, Vuong THP, Huynh DT. Max–min Dcluster formation in wireless ad hoc networks, in Proc. IEEE INFOCOM, Tel-Aviv, Israel. 2000; 32.
7. Liu X, Cao J, Lai S, Yang C, Wu H, Xu Y. Energy efficient clustering for WSN-based structural health monitoring, in Proc. IEEEINFOCOM. 2011; 2768.
8. Zhang Z, Ma M, Yang Y. Energy efficient multi-hop polling in clusters of two-layered heterogeneous sensor networks,IEEE Trans. Comput.2008; 57(2): 231.
9. Kun S, An L, Peng N, Douglas M. Securing network access in wireless sensor networks, in Proc. 2009 International Conference onWireless Network Security. 261.
10. *Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, Tygar JD. SPINS: Security Protocols for Sensor Networks. Department of Electrical Engineering and Computer Sciences University of California, Berkeley.*
11. CasadoL, Tsigas P. Contikisec: a secure network layer for wireless sensor networks under the Contiki operating system, in Proc. 2009Nordic Conference on Secure IT Systems. 133–147.
12. Hwang JJ, Shao BM, Wang PC. A new access control method using prime factorization, The Computer. 1992; 35(1): 16.
13. Yu CM, Tsou YT, Lu CS, Kuo SY. Constrained functionbased message authentication for sensor networks,IEEE Trans. Inf.Forensic and Security.2011; 6(2): 407.
14. Lu L, He T, Abdelzaher T, Stankovic J. Design and comparison of lightweight group management strategies in EnviroSuite, in Proc. International Conference on Distributed Computing in SensorNetworks.2005; 155.
15. *MiaoZhao, Yuanyuan Yang. Bounded Relay Hop Mobile Data Gathering in Wireless Sensor Networks Department of Electrical and Computer Engineering, State University of New York, Stony Brook, NY 11794, US.*
16. Perrig A, Szewczyk R, Wen V, Culler D, Tygar JD. SPINS: security protocols for sensor networks, in Proc. InternationalConference on Mobile Computing and Networking. 2001; 189.
17. Karlof C, Sastry N, Wagner D. TinySec: a link layer security architecture for wireless sensor networks, in Proc. InternationalConference on Embedded Networked Sensor Systems.2004; 162.
18. ZigBee Alliance, Zigbee specifications, Technical Report Document 053474r06. 2005.
19. Luk M, Mezzour G, Perrig A, Gligor V. MiniSec: a secure sensor network communication architecture, in Proc. InternationalConference on Information Processing in Sensor Networks. 2007; 479.
20. Ganeriwal S, Capkun S, Srivastava MB. Secure time synchronization in sensor networks, ACM Trans. Inf. and Systems Security.2006; 11(4): 1.

Source of support: Nil, Conflict of interest: None Declared