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

A Novel Design for Safeguarding Network Aggregation by Identifying False Temporal Variation Patterns

Singurusantosh
M.Tech (software engineering),
Department of Computer Science and Engineering,
Sarada Institute of Science Technology
and Mangement, Srikakulam.

Ramesh kumarBehara
Assistant Professor,
Department of Computer Science and Engineering,
Sarada Institute of Science Technology and
Mangement, Srikakulam.

Abstract:

A wireless sensor network (WSN) of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. Wireless sensor networks are installed in a lot of intimidating and unfriendly atmospheres and countenance numerous security issues. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.Sensor nodes are also resource-constrained.

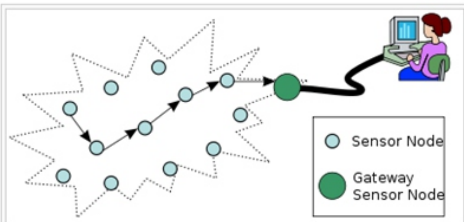
In present wireless networks are using in many applications. In The security issues for example, information honesty, secrecy, and freshness in information collection get to be significant when the WSN is conveyed in a remote or unfriendly environment where sensors are inclined to hub disappointments and bargains. There is right now scrutinizing potential in securing information collection in the WSN. The most existing aggregation algorithms and systems do not include any provisions for providing security, and consequently these systems are vulnerable to a large variety of attacks.

Because of this, the security issues in information collection for the WSN will be examined in this paper. So we introduced a simple and efficient method for using quotient and reminder method for secure sharing of keys and local authentication at aggregator nodes. In this we used symmetric cryptographic techniques avoids key sharing and secure exchanging of data.

Keywords: Wireless Sensor networks, aggregation, security, Cryptography, sensors, energy consumption, Authentication, Keys, Communications.

Introduction:

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

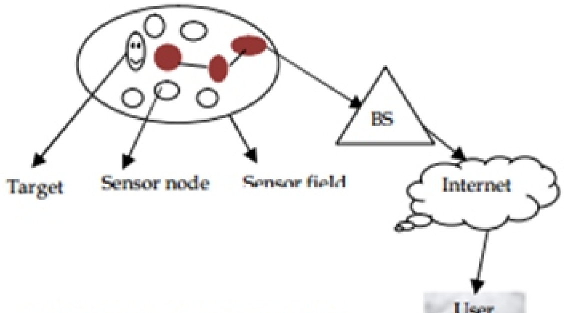


Typical multi-hop wireless sensor network architecture

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

The main characteristics of a WSN include:

- Power consumption constraints for nodes using batteries or energy harvesting.
- Ability to cope with node failures (resilience).
- Mobility of nodes.
- Heterogeneity of nodes.
- Scalability to large scale of deployment.
- Ability to withstand harsh environmental conditions.
- Ease of use.
- Cross-layer design.



Architecture of the Sensor network

Clustering In WSN:

Sensor node are densely deployed in wireless sensor network that means physical environment would produce very similar data in close by sensor node and transmitting such type of data is more or less redundant. So all these facts encourage using some kind of grouping of sensor nodes such that group of sensor node can be combined or compress data together and transmit only compact data. This can reduce localized traffic in individual group and also reduce global data. This grouping process of sensor nodes in a densely deployed large scale sensor node is known as clustering. The way of combing data and compress data belonging to a single cluster called data fusion (aggregation). Issues of clustering in wireless sensor network:-

1. How many sensor nodes should be taken in a single cluster.Selection procedure of cluster head in an individual cluster.

2. Heterogeneity in a network, it means user can put some power full nodes, in term of energy in the network which can behave like cluster head and simple node in a cluster work as a cluster member only. Many protocols and algorithm have been proposed which deal with each individual issue.

Nowadays, wireless sensor networks (WSNs) are increasingly used in critical applications within several fields including military, medical and industrial sectors. Given the sensitivity of these applications, sophisticated security services are required. Key management is a corner stone for many security services such as confidentiality and authentication which are required to secure communications in WSNs. The establishment of secure links between nodes is then a challenging problem in WSNs. Because of resource limitations, symmetric key establishment is one of the most suitable paradigms for securing exchanges in WSNs.

On the other hand, because of the lack of infrastructure in WSNs, we have usually no trusted third party which can attribute pairwise secret keys to neighboring nodes, that is why most existing solutions are based on key pre-distribution. Over the last decade, a host of research work dealt with symmetric key predistribution issue for WSNs and many solutions have been proposed in the literature.

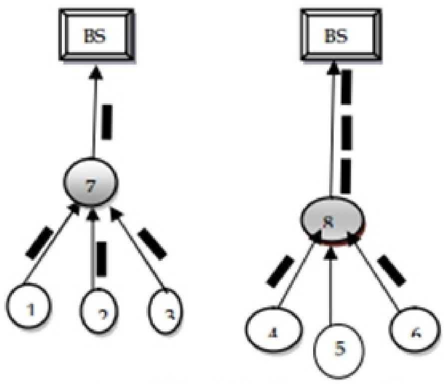
Nevertheless, in most existing solutions, the design of key rings (blocks of keys) is strongly related to the network size, these solutions either suffer from low scalability (number of supported nodes), or degrade other performance metrics including secure connectivity, storage overhead and resiliency in the case of large networks.

Data Aggregation :

In typical wireless sensor networks, sensor nodes are usually resource-constrained and battery-limited. In order to save resources and energy, data must be aggregated to avoid overwhelming amounts of traffic in the network. There has been extensive work on data aggregation schemes in sensor networks, The aim of data aggregation is that eliminates redundant data transmission and enhances the lifetime of energy in wireless sensor network. Data aggregation is the process of one or several sensors then collects the detection result from other sensor.

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

The collected data must be processed by sensor to reduce transmission burden before they are transmitted to the base station or sink. The wireless sensor network has consisted three types of nodes. Simple regular sensor nodes, aggregator node and querier. Regular sensor nodes sense data packet from the environment and send to the aggregator nodes basically these aggregator nodes collect data from multiple sensor nodes of the network, aggregates the data packet using a some aggregation function like sum, average, count, max min and then sends aggregates result to upper aggregator node or the querier node who generate the query.



Data aggregation model and Non data aggregation model

It can be the base station or sometimes an external user who has permission to interact with the network. Data transmission between sensor nodes, aggregators and the querier consumes lot of energy in wireless sensor network.

Figure contain two models one is data aggregation model and second is non data aggregation model in which sensor nodes 1, 2, 3,4,5,6 are regular nodes that collecting data packet and reporting them back to the upper nodes where sensor nodes 7,8 are aggregators that perform sensing and aggregating at the same time. In this aggregation model 4 data packet travelled within the network and only one data packet is transmitted to the base station (sink).

And other non data aggregation model also 4 data packet travelled within the network and all data packets are sent to the base station(sink), means we can say that with the help of data aggregation process we decrease the number of data packet transmission. And also save energy of the sensor node in the wireless sensor network.

With the help of data aggregation we enhance the lifetime of wireless sensor network. Sink have a data packet with energy efficient manner with minimum data latency. So data latency is very important in many applications of wireless sensor network such as environment monitoring, health, monitoring, where the freshness of data is also an important factor. It is critical to develop energy-efficient data-aggregation algorithms so that network lifetime is enhanced.

There are several factors which determine the energy efficiency of a sensor network, such as network architecture, the data-aggregation mechanism, and the underlying routing protocol. Wireless sensor network has distributed processing of sensor node data. Data aggregation is the technique.

It describes the processing method that is applied on the data received by a sensor node as well as data is to be routed in the entire network. In which reduce energy consumption of the sensor nodes and also reduce the number of transmissions or length of the data packet. Elena Fosolo et al in describe "In network aggregation is the exclusive process of collecting and routing information through a multi hop network. Processing of data packet with the help of intermediate sensor nodes.

The objective of this approach is increasing the life time of the network and also reduces resource consumption. There are two type of approach for in network aggregation. With size reduction and without size reduction .In network aggregation with size reduction. It is the process in which combine and compressing the data received by a sensor node from its neighbors in order to reduce the length of data packet to be sent towards the base station.

Example, in some circumstance a node receives two data packets which have a correlated data. In this condition it is useless to send both data packets. Then we apply a function like MAX, AVG, and MIN and again send single data packet to base station. With help of this approach we reduce the number of bit transmitted in the network and also save a lot of energy. In network aggregation without size reduction is defined in the process of data packets received by different neighbors in to a single data packet but without processing the value of data. This process also reduces energy consumption or increase life time of the network.

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

Providing security to aggregate data in Wireless Sensor Networks is known as Secure Data Aggregation in WSN.were the first few works discussing techniques for secure data aggregation in Wireless Sensor Networks.Two main security challenges in secure data aggregation are confidentiality and integrity of data.

While traditionally encryption is used to provide end to end confidentiality in Wireless Sensor Network (WSN), the aggregators in a secure data aggregation scenario need to decrypt the encrypted data to perform aggregation. This exposes the plaintext at the aggregators, making the data vulnerable to attacks from an adversary. Similarly an aggregator can inject false data into the aggregate and make the base station accept false data. Thus, while data aggregation improves energy efficiency of a network, it complicates the existing security challenges.

Existing System:

Several secure hierarchical aggregation schemes follow an aggregation-commitment-attest framework. During the in-network aggregation, each node computesthe hash as commitment over the input of its aggregationcomputation, intermediate results, and data commitmentsfrom its children, and then sends the hash to its parent.Based on the commitments, interactive attest is performedbetween the base station and sensor nodes when aggregationcompletes.

Some researchers propose a secure hop-by-hopdata aggregation protocol SDAP. The tree topology ispartitioned into multiple logical subtreegroups, and sensordata are aggregated in every subtree separately to reducethe trust on high-level nodes.

Disadvantages:

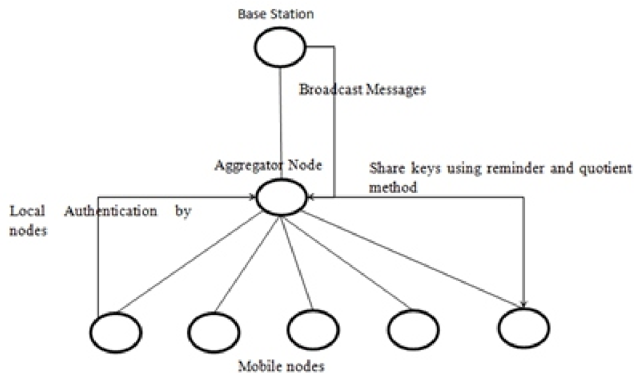
1.By using of asymmetric techniques there is a chance to leak data.

2.By using of level aggregation techniques the total process of broadcasting become very complex to base station.

3.Authentication methods are not much strong to verify users.

Proposed System:

We proposed an architecture that consists of three objects such as base station, aggregator node, and mobile nodes. In this uses symmetric technique to provide authentication to mobile users. The architecture is shown below:



In this the base station broadcasts the messages to mobile through aggregator node.

Aggregator node authenticates the mobile nodes because of the protection of the nodes from malicious users and this is so called as local authentication. For mobile nodes , for the purpose of authenticity we proposed simple and efficient method that is reminder and quotient method which avoids key sharing.

Initial setup phase:

Initially mobile nodes register themselves at base station and base station allots unique Id and nonce (sk) value to mobile node. Then aggregate node generates a random numbers for all mobiles nodes connected to base station such as R={r1,r2,r3…rn}. These random numbers are converted by using reminder and quotient method as shown below key setup phase:

Key Setup phase:

Step1: Random numbers R={r1,r2,r3,…rn}, nonce=sk
Step2: For every user
Q=r1/sk
R=r1%sk
QBinary=Binary(Q)
RBinary=Binary(R)

```
Binary(N):
intnum;
num = N;
intquot;
string rem = “”;
while (num>= 1)
      {
quot = num / 2;
rem += (num % 2).ToString();
num = quot;
      }
   // Reversing the  value
string bin = “”;
for (int i = rem.Length - 1; i >= 0; i--)
      {
bin = bin + rem[i];
      }
```

This binary value of reminder and quotient is send to mobile nodes. The aggregate node sends the sum of the random numbers generated to the base station.
The mobile regenerate the random number using the binary formatted reminder and quotient as shown below:

r=(B(Q) * B(sk))+B(r)

after this authentication step,

Local Authentication phase:

In this phase we aggregate node collects all retrieved random numbers and find aggregation of these random numbers

Ag(R)=∑ r mod N;

This value sent to the base station , then BS checks this aggregation and confirms all mobile nodes are authenticated then it broadcasts the message to mobile node using symmetric encryption technique.First we translate all of our characters to numbers, ‘a’=0, ‘b’=1, ‘c’=2, ... , ‘z’=25. We can now represent the Caesar cipher encryption function, e(x), where x is the character we are encrypting, as:

$$e(x) = (x + k) \pmod{26}$$

Where k is the key (the shift) applied to each letter. After applying this function the result is a number which must then be translated back into a letter. The decryption function is :

$$e(x) = (x - k) \pmod{26}$$

Conclusion:

In this paper we examined unique outline issues non-stop collection in WSNs. A proficient check plan is proposed to secure the legitimacy of the transient variety designs in the total results. Contrasted and the current secure total plans our plan just need to check a little partition of collection brings about a period window and, therefore, incredibly diminishes the confirmation cost. We characterize agent focuses and propose relating calculations for delegate point choice. By utilizing our proposed framework we lessen handling time and build effectiveness.

References:

[1] Lei Yu, Member, IEEE, Jianzhong Li, Member, IEEE, Siyao Cheng, ShuguangXiong, and HaiyingShen, Member, IEEE, Secure Continuous Aggregation in Wireless Sensor Networks, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 3, MARCH 2014.

[2] Wireless sensor networks: a survey I.F. Akyildiz, W. Su*, Y.Sankarasubramaniam, E. Cayirci Broadband and WirelessNetworking Laboratory, School of Electrical and ComputerEngineering, Georgia Institute of Technology, Atlanta, GA30332, USA.

[3] Data Aggregation in Wireless Sensor Network Nandini. S.Patil, Prof. P. R. Patil B.V. Bhoomaraddi College of Engineering and Technology, Hubli 580031, India,Visvesvaraiya Technological University Belgum-590014, India.

[4] D. Estrin, R. Govindan, J. Heidemann, S. Kumar, Next centurychallenges: scalable coordination in sensor networks, ACMMobiCom’99, Washingtion, USA, 1999, pp. 263–270.

[5] J. Agre, L. Clare, An integrated architecture for cooperativesensing networks, IEEE Computer Magazine (May 2000)106–108.

[6] M. Bhardwaj, T. Garnett, A.P. Chandrakasan, Upper bounds onthe lifetime of sensor networks, IEEE International Conferenceon Communications ICC’01, Helsinki, Finland, June 2001.

[7] P. Bonnet, J. Gehrke, P. Seshadri, Querying the physical world,IEEE Personal Communications (October 2000) 10–15.

[8] N. Bulusu, D. Estrin, L. Girod, J. Heidemann, and ScalableCoordination for wireless sensor networks: self-configuringlocalization systems, International Symposium onCommunication Theory and Applications (ISCTA 2001), Ambleside, UK, July 2001.

[9] A. Cerpa, D. Estrin, ASCENT: adaptive self-configuring Sensor networks topologies, UCLA Computer ScienceDepartment Technical Report UCLA/CSDTR-01-0009, May 2001.

[10] A. Cerpa, J. Elson, M. Hamilton, J. Zhao, and Habitat monitoring: application driver for wireless communications technology, ACM SIGCOMM'2000, Costa Rica, April 2001.

[11] S. Cho, A. Chandrakasan, Energy-efficient protocols for Lowduty cycle wireless micro sensor, Proceedings of the 33rdAnnual Hawaii International Conference on System Sciences,Maui, HI Vol. 2 (2000), p. 10.

[12] C. Intanagonwiwat, R. Govindan, D. Estrin, Directed diffusion:a scalable and robust communication paradigm for sensornetworks, Proceedings of the ACM Mobi- Com'00, Boston,MA, 2000, pp. 56–67.

[13] C. Jaikaeo, C. Srisathapornphat, C. Shen, Diagnosis of sensornetworks, IEEE International Conference on CommunicationsICC'01, Helsinki, Finland, June 2001.

[14] B. Warneke, B. Liebowitz, K.S.J. Pister, Smart dust: communicating with a cubic-millimeter computer, IEEE Computer (January 2001) 2–9.

[15] http://www.fao.org/sd/EIdirect/EIre0074.htm.

[16] J.M. Kahn, R.H. Katz, K.S.J. Pister, Next century challenges:mobile networking for smart dust, Proceedings of the ACMMobiCom'99, Washington, USA, 1999, pp. 271–278.

[17] N. Noury, T. Herve, V. Rialle, G. Virone, E. Mercier, G.Morey, A. Moro, T. Porcheron, Monitoring behavior in homeusing a smart fall sensor, IEEE-EMBS Special Topic Conference on Micro technologies in Medicine and Biology. October 2000, pp. 607–610.

[18] E.M. Petriu, N.D. Georganas, D.C. Petriu, D. Makrakis, V.Z.Groza, Sensor-based information appliances, IEEE Instrumentation and Measurement Magazine (December 2000)31–35.

[19] D. Nadig, S.S. Iyengar, A new architecture for distributedsensor integration, Proceedings of IEEE Southeastcon'93,Charlotte, NC, and April 1993.

[20] C. Shen, C. Srisathapornphat, C. Jaikaeo, Sensor informationnetworking architecture and applications, IEEE PersonalCommunications, August 2001, pp. 52–59.